StringFlix School Privacy Policy (Educational Account)

1. Introduction

At StringFlix School (“we”, “us”, “our”), our mission is to establish a more meaningful social experience by creating collaborative video content. We have developed policies and procedures to ensure that StringFlix School is a safe environment for our users (“customers”, “you”, “your”) to create and share information. Central to ensuring a safe environment is the protection of our customers’ private information. This Privacy Policy outlines how we collect, use, share, and store your data, as well as the procedures we put in place to ensure that your confidential information is protected from unauthorized access and complies with all applicable privacy legislation.

2. Regulatory Compliance

StringFlix School complies with Ontario’s privacy laws to prevent third-parties from gaining unauthorized access to Customer information, including *the Personal Information Protection and Electronic Documents Act (PIPEDA)* and the *Freedom of Information and Protection of Privacy Act (FIPA)*. StringFlix School protects the personal information of minors in compliance with the *Municipal Freedom of Information and Protection of Privacy Act* (*MFIPPA*), Revised Statutes of Ontario 1990, chapter M.56 for customers to whom it applies. It is the customer’s responsibility to ensure that the services provided by StringFlix School are in compliance with any legal obligations under *MFIPPA*. StringFlix School requires parental consent for minors 16 years of age or younger to use the platform.

3. Data Collection

StringFlix School requires the collection of customer information in order to provide customers with access to the platform and engage with the provided services. Data is also collected for the purposes of improving the platform, marketing, and customer service. This data is processed by StringFlix School only in accordance with the purposes to which you have provided consent. StringFlix School will ensure that the collected information is stored securely. StringFlix School will disclose any breaches to secure information as governed by the local applicable law.

3.1 Type of Information Collected

StringFlix School collects personal information from customers, which includes names, pictures, videos, school, email addresses, device information and other log data pertaining to the use of our platform. StringFlix School aims to limit data collection to only that required to perform its services.

StringFlix School may aggregate customer personal information that will be anonymized, ensuring that the customer is not identifiable. Such aggregate data will be used for analyzing trends for the purposes of marketing and improving the platform. By providing personal information to StringFlix School, the customer agrees and consents to the use of such information in aggregate form.

4. Use of Customer Information

StringFlix School collects customer information for the following purposes:

- Communication with customers to provide information regarding updates, services, or notifications;
- Provide our customers with customer support;
- To allow customers to access and use the StringFlix School platform;
- To allow customers to share content using the StringFlix School platform; and
- To analyze customer trends for improving and developing the services provided by StringFlix School.

StringFlix School may use third-party services for the purpose of developing and improving the platform and services (e.g., Google Analytics).

5. Sharing and disclosure of information

StringFlix School recognizes that the protection of your personal information is of the utmost importance and will only disclose and share this information, in part or in whole, as described in this section.

We will only share your information with third parties who are not our partners in the following situations:

- With your explicit consent;
- Where we have a good faith belief that access, use, preservation or disclosure of your personal information is reasonably necessary to (a) satisfy any applicable law, regulation or government request, (b) enforce terms and conditions of this privacy policy, (c) protect, prevent and address fraud, security or technical issues, (d) protect against harm to the rights, property or safety of us, our customers or the public as required or permitted by law.

StringFlix School will not share any personal information without first obtaining customer consent or as otherwise required by law. The customer may withdraw consent to the use of such information at any time. Withdrawal of consent will result in reduced access to the StringFlix School platform and use of the provided services.

StringFlix School may enable you to share information with other customers. Once you share this information with other customers, you should be aware that those customers may share that information at their discretion.

Except as a sale of all or substantially all of our assets, StringFlix School does not sell, rent, trade, in part or in whole, your personal information, without your consent, to third parties who are not partners. StringFlix School will never sell your information, in part or in whole, to advertisers. We will not disclose any customer information for behavioral targeting of advertisements.

6. Protection of Information

We strive to keep your personal information safe and secure. StringFlix School believes that the security of your information is of the highest concern. We will take appropriate security measures to protect against unauthorized access to or unauthorized alteration, disclosure or destruction of personal information. Your personal information is only accessible to StringFlix School employees, contractors and agents who are required to know that information in order to process it on our behalf. All of these individuals are bound by confidentiality obligations and may be subject to civil and criminal actions if they fail to uphold these obligations.

StringFlix School implements various security measures to ensure that all stored personal information is secure and safe. Here are some of the things we do to keep your data secure by leveraging Amazon Simple Storage Service (S3) via Amazon Web Services (AWS):

Data Centers

AWS data centers are state of the art, utilizing innovative architectural and engineering approaches. Amazon has many years of experience in designing, constructing, and operating large-scale data centers. This experience has been applied to the AWS platform and infrastructure. AWS data centers are housed in facilities that are not branded as AWS facilities.

Redundancy

Amazon S3 is designed to provide 99.999999999% durability and 99.99% availability of objects over a given year. Objects are redundantly stored on

multiple devices across multiple facilities in an Amazon S3 region. To help provide durability, Amazon S3 PUT and COPY operations synchronously store customer data across multiple facilities before returning SUCCESS. Once stored, Amazon S3 helps maintain the durability of the objects by quickly detecting and repairing any lost redundancy. Amazon S3 also regularly verifies the integrity of data stored using checksums. If corruption is detected, it is repaired using redundant data. In addition, Amazon S3 calculates checksums on all network traffic to detect corruption of data packets when storing or retrieving data.

Power

The data center electrical power systems are designed to be fully redundant and maintainable without impact to operations, 24 hours a day, and seven days a week. Uninterruptible Power Supply (UPS) units provide back-up power in the event of an electrical failure for critical and essential loads in the facility. Data centers use generators to provide back-up power for the entire facility.

Server Operating System

Amazon's Corporate Applications team develops and manages software to automate IT processes for UNIX/Linux hosts in the areas of third-party software delivery, internally developed software, and configuration management. The Infrastructure team maintains and operates a UNIX/Linux configuration management framework to address hardware scalability, availability, auditing, and security management. By centrally managing hosts through the use of automated processes that manage change, Amazon is able to achieve its goals of high availability, repeatability, scalability, security, and disaster recovery.

Business Continuity

Amazon's infrastructure has a high level of availability and provides StringFlix School the features to deploy a resilient IT architecture. AWS has designed its systems to tolerate system or hardware failures with minimal customer impact. Data center Business Continuity Management at AWS is under the direction of the Amazon Infrastructure Group.

Data Transmission

For maximum security, StringFlix School's data is securely uploaded/downloaded to Amazon S3 via the SSL encrypted endpoints. The encrypted endpoints are accessible from both the Internet and from within Amazon EC2, so that data is transferred securely both within AWS and to and from sources outside of AWS.

Intrusion Detection

AWS uses a wide variety of automated monitoring systems to provide a high level of service performance and availability. AWS monitoring tools are designed to detect unusual or unauthorized activities and conditions at ingress and egress communication points. These tools monitor server and network usage, port scanning activities, application usage, and unauthorized intrusion attempts. The tools have the ability to set custom performance metrics thresholds for unusual activity.

Systems within AWS are extensively instrumented to monitor key operational metrics. Alarms are configured to automatically notify operations and management personnel when early warning thresholds are crossed on key operational metrics.

Incident Response

An on-call schedule is used so personnel are always available to respond to operational issues. This includes a pager system so alarms are quickly and reliably communicated to operations personnel.

The Amazon Incident Management team employs industry-standard diagnostic procedures to drive resolution during business-impacting events. Staff operators provide 24x7x365 coverage to detect incidents and to manage the impact and resolution.

Site Control

Physical access is strictly controlled both at the perimeter and at building ingress points by professional security staff utilizing video surveillance, intrusion detection systems, and other electronic means.

Authorized staff must pass two-factor authentication a minimum of two times to access data center floors. All visitors are required to present identification and are signed in and continually escorted by authorized staff.

AWS only provides data center access and information to employees and contractors who have a legitimate business need for such privileges. When an employee no longer has a business need for these privileges, his or her access is immediately revoked, even if they continue to be an employee of Amazon or

Amazon Web Services. All physical access to data centers by AWS employees is logged and audited routinely.

Access Control for AWS Personnel

The AWS Production network containing StringFlix School is segregated from the Amazon Corporate network and requires a separate set of credentials for logical access. The Amazon Corporate network relies on user IDs, passwords, and Kerberos, whereas the AWS Production network requires SSH public-key authentication through a bastion host.

AWS developers and administrators on the Amazon Corporate network who need to access AWS cloud components must explicitly request access through the AWS access management system. All requests are reviewed and approved by the appropriate owner or manager.

Internal Data Access Processes and Policies

AWS has established formal policies and procedures to delineate the minimum standards for logical access to AWS platform and infrastructure hosts. AWS conducts criminal background checks, as permitted by law, as part of pre-employment screening practices for employees and commensurate with the employee's position and level of access. The policies also identify functional responsibilities for the administration of logical access and security.

Accounts are reviewed every 90 days; explicit re-approval is required or access to the resource is automatically revoked. Access is also automatically revoked when an employee's record is terminated in Amazon's Human Resources system. Windows and UNIX accounts are disabled and Amazon's permission management system removes the user from all systems.

Requests for changes in access are captured in the Amazon permissions management tool audit log. When changes in an employee's job function occur, continued access must be explicitly approved to the resource or it will be automatically revoked.

AWS Security has established a credentials policy with required configurations and expiration intervals. Passwords must be complex and are forced to be changed every 90 days.

Access Control and Privilege Management

When you first create a DB Instance within Amazon RDS, you will create a master user account, which is used only within the context of Amazon RDS to control access to your DB Instance(s). The master user account is a native database user account that allows you to log on to your DB Instance with all database privileges. You can specify the master user name and password you want associated with each DB Instance when you create the DB Instance. Once you have created your DB Instance, you can connect to the database using the master user credentials. Subsequently, you can create additional user accounts so that you can restrict who can access your DB Instance.

You can control Amazon RDS DB Instance access via DB Security Groups, which are similar to Amazon EC2 Security Groups but not interchangeable. DB Security Groups act like a firewall controlling network access to your DB Instance. Database Security Groups default to a “deny all” access mode and customers must specifically authorize network ingress. There are two ways of doing this: authorizing a network IP range or authorizing an existing Amazon EC2 Security Group. DB Security Groups only allow access to the database server port (all others are blocked) and can be updated without restarting the Amazon RDS DB Instance, which allows a customer seamless control of their database access.

Using AWS IAM, you can further control access to your RDS DB instances. AWS IAM enables you to control what RDS operations each individual AWS IAM user has permission to call.

Audits and Certifications

The IT infrastructure that AWS provides StringFlix School is designed and managed in alignment with security best practices and a variety of IT security standards, including: SOC 1/SSAE 16/ISAE 3402 (formerly SAS 70), SOC 2, SOC 3, FISMA, DIACAP, and FedRAMP, DOD CSM Levels 1-5, PCI DSS Level 1, ISO 9001 / ISO 27001 / ISO 27017 / ISO 27018, ITAR, FIPS 140-2, MTCS Level 3 and HITRUST

Data Storage, Isolation and Authentication

Amazon S3 thoroughly protects data at rest. StringFlix School uses Amazon S3 Server-Side Encryption (SSE). Data is encrypted with a key generated by AWS or with a key you supply, depending on your requirements. With Amazon S3 SSE, you can encrypt data on upload simply by adding an additional request header when writing the object. Decryption happens automatically when data is retrieved. Amazon S3 SSE uses one of the strongest block ciphers available – 256-bit Advanced Encryption Standard (AES-256). With Amazon S3 SSE, every

protected object is encrypted with a unique encryption key. This object key itself is then encrypted with a regularly rotated master key. Amazon S3 SSE provides additional security by storing the encrypted data and encryption keys in different hosts. Amazon S3 SSE also makes it possible for you to enforce encryption requirements.

Different instances running on the same physical machine are isolated from each other via the Xen hypervisor. Amazon is active in the Xen community, which provides awareness of the latest developments. In addition, the AWS firewall resides within the hypervisor layer, between the physical network interface and the instance's virtual interface. All packets must pass through this layer, thus an instance’s neighbors have no more access to that instance than any other host on the Internet and can be treated as if they are on separate physical hosts. The physical RAM is separated using similar mechanisms.

AWS customer instances have no access to raw disk devices, but instead are presented with virtualized disks. The AWS proprietary disk virtualization layer automatically resets every block of storage used by the customer, so that one customer’s data is never unintentionally exposed to another. In addition, memory allocated to guests is scrubbed (set to zero) by the hypervisor when it is unallocated to a guest. The memory is not returned to the pool of free memory available for new allocations until the memory scrubbing is complete.

While we do not guarantee the security of your personal information, we will make best efforts to reduce the risk of misuse or unauthorized access to your personal information. You are responsible for keeping your passwords secret and for using proper security habits to keep that information secure.

7. Breach of information

We strive to protect your personal information from unauthorized access and disclosure. To the extent that provincial or federal laws apply to a security breach, StringFlix School will comply with the applicable law. In the event that no such law applies to a security breach, StringFlix School will notify you in the most expedient time possible, without unreasonable delay, and after determining the extent of the breach and restoring the integrity of the system. We will also make reasonable efforts to ensure the breach is contained and restore the integrity of the system.

For the purpose of this section, a security breach means an actual disclosure, or a reasonable belief that there has been a disclosure of personal information to any unauthorized entity.

8. Deletion of information

All accounts, including all personal information contained within, are automatically deleted one year after the accounts expiry or at any time upon a customer's request. Upon deletion of your account, StringFlix School will destroy, in part and in whole, all copies of your personal information, as well as pointers to this data and ensure this information is not recoverable or restorable by StringFlix School on all of its active and replication servers. Accounts that are inactive for over a one year are deemed to have expired.

Parents may delete the account of any of their children if they are less than 16 years old.

9. Rectification of information

Customers have access to their personal details within their accounts and can modify this information at their discretion. If you come across incorrect information, you have the right to submit a request to modify this information.

Parents may modify information found within the account of any of their children if they are less than 16 years old.

10. Access and Modification of information

Customers can submit a request to view, all or part, of the personal information collected by StringFlix School about them. StringFlix School will endeavor to provide this information within a reasonable timeframe or as required by law.

StringFlix School may refuse to provide you access to your personal information if you do not provide sufficient information to verify your identity, if we deem the request, in our sole discretion, to be unreasonable in the circumstances, or as otherwise provided by legislation.

11. Modification of this Policy

We plan on regularly reviewing our Privacy Policy. We reserve the right to modify this policy at any time. Should we modify this policy, we will send you an email and post an update on our website. It is possible in the future that StringFlix School could merge with, or be acquired by another company. In that case, you consent to the resulting company having access to the personal information maintained by StringFlix School. The resulting company would be bound by this Privacy Policy unless it modifies it and notifies you.

12. Data Transfer

All of our customer's personal information is stored within Canada. Your personal information will not be transferred to another jurisdiction without your consent.

13. General Consent

We recommend that you carefully read our Privacy Policy because your use of StringFlix School implies consent to its terms and conditions. Should you disagree with any terms of this Privacy Policy, StringFlix School should not be used.

14. Contact

We strive to make our Privacy Policy as easy to understand as possible. If you have any questions, comments or concerns about this Privacy Policy, the data that we collect or how it is being used, or to report suspected misuse of that data, please contact us at sales@StringFlix School.com.