

Data Sharing/Use Agreement
Between
Jefferson County Board of Education
And
SoftChalk, LLC

This Data Sharing/Use Agreement ("Agreement") between the Jefferson County Board of Education, a political subdivision of the Commonwealth of Kentucky doing business as the Jefferson County Public Schools ("JCPS"), and SoftChalk, LLC, a Virginia limited liability company organized under the laws of Virginia. ("Services Provider") describes the services to be provided to JCPS by Services Provider, and the means to be used by Services Provider to ensure the confidentiality and security of information and data exchanged between JCPS and Services Provider in connection with the provision of the services.

A. PERIOD OF THE AGREEMENT

This Agreement shall be effective as of May 25, 2022 and will terminate when the services contract referenced in Paragraph B.1. below terminates, unless terminated earlier by either party pursuant to Section H.

B. SCOPE OF THE AGREEMENT AND INTENDED USE OF THE DATA

1. Services Provider will provide the following services to JCPS under the terms of a services contract between JCPS and Services Provider effective May 25, 2022: SoftChalk is a content authoring tool and learning object repository which campus instructors use to create presentations and learning modules inclusive of quizzes and other types of practice assignments.
2. JCPS and Services Provider agree that Services Provider is an organization to which JCPS can disclose, personally identifiable information from an education record of a student, as defined in 34 CFR 99.3, under the "school official exception" of the Family Educational Rights and Privacy Act, 20 U.S.C. 1232(g) and 34 C.F.R. 99.31 (a)(1) ("FERPA"), because the disclosure is to a contractor to whom JCPS has outsourced institutional services or functions for which JCPS would otherwise use employees; the contractor is under the direct control of JCPS with respect to the use and maintenance of education records; and the contractor is subject to the requirements of 34 CFR 99.33(a) governing the use and redisclosure of personally identifiable information from education records.
3. JCPS shall disclose to Services Provider, confidential, personally identifiable information from an education record of a student, as defined in 34 C.F.R. 99.3,

under the "school official exception" of FERPA, 34 C.F.R. 99.31 (a)(1), when the disclosure is within such exception as stated in Paragraph B.2 above and Services Provider has a legitimate educational interest for access to such education records. The confidential data, including student and non-student information to be disclosed, is described in a document attached to this agreement as **Attachment A**. Services Provider shall use personally identifiable information from education records and other records in order to perform the services described in Paragraph B.1 above. Services Provider shall notify JCPS and JCPS shall provide written consent, if approved, of any changes to the list of disclosed data necessary for the services or any changes to the scope, purpose or duration of the services themselves. Any agreed upon changes to the data disclosed shall be reduced to writing and included in an update to Attachment A to this Agreement. Any agreed upon changes to the scope, purpose or duration of the services shall be reduced to writing and included in an amendment to the services contract described in Paragraph B.1 above.

4. Services Provider and JCPS shall work cooperatively to determine the proper medium and method for the transfer of confidential data between each other. Services Provider shall confirm the transfer of confidential data and notify JCPS as soon as practicable of any discrepancies between the actual data transferred and the data described in this Agreement. The same protocol shall apply to any transfer of confidential data from Services Provider to JCPS.

C. CONSTRAINTS ON USE OF DATA

1. Services Provider agrees that the services shall be provided in a manner that does not permit personal identification of parents and students by individuals other than representatives of Services Provider that have legitimate interests in the information.
2. Services Provider will not contact the individuals included in the data sets without obtaining advance written authorization from JCPS.
3. Services Provider shall not re-disclose any individual-level data with or without identifying information to any other requesting individuals, agencies, or organizations without prior written authorization by JCPS.
4. Services Provider shall use the data only for the purpose described in Paragraph B.1 above. The data shall not be used for personal gain or profit.

D. DATA CONFIDENTIALITY AND DATA SECURITY

Services Provider agrees to the following confidentiality and data security statements:

1. Services Provider acknowledges that the data is confidential data and proprietary to JCPS, and agrees to protect the data from unauthorized disclosures and to comply with all applicable Local, State and Federal confidentiality laws and regulations including but not limited to FERPA; the Kentucky Family Educational

Rights and Privacy Act, KRS 160.700 et seq.; the Richard B. Russell National School Lunch Act, 42 U.S.C. 1751 et seq.; the Child Nutrition Act of 1966, 42 U.S.C. 1771 et seq.; 7 C.F.R. 245.6 et seq.; the Personal Information Security and Breach Investigation Procedures and Practices Act, KRS 61.931 et seq.; and the Kentucky Open Records Act, KRS 61.820 et seq.

2. If the performance of this Agreement involves the transfer by JCPS to Services Provider of any data regarding any JCPS student that is subject to FERPA, Services Provider agrees to:
 - a. In all respects comply with the provisions of FERPA.
 - b. Use any such data for no purpose other than to fulfill the purposes of the services contract described in Paragraph B.1 above, and not share any such data with any person or entity other than Services Provider and its employees, contractors and agents, without the prior written approval of JCPS.
 - c. Require all employees, contractors and agents of Services Provider to comply with all applicable provisions of FERPA with respect to any such data.
 - d. Maintain any such data in a secure computer environment, and not copy, reproduce or transmit any such data except as necessary to fulfill the purposes of the services contract described in Paragraph B.1 above.
 - e. Provide the services under the services contract described in Paragraph B.1 above in a manner that does not permit the identification of an individual student by anyone other than employees, contractors or agents of Services Provider having a legitimate interest in knowing such personal identification.
 - f. Destroy or return to JCPS any such data obtained under this Agreement within thirty days (30) after the date within it is no longer needed by Services Provider for the purposes of the services contract described in Paragraph B.1 above.
3. Services Provider shall not release or otherwise reveal, directly or indirectly, the data to any individual, agency, entity, or third party not included in this Agreement, unless such disclosure is required by law or court order. If Services Provider becomes legally compelled to disclose any confidential and otherwise personally identifiable data (whether by judicial or administrative order, applicable law, rule or regulation, or otherwise), then Services Provider shall use all reasonable efforts to provide JCPS with prior notice before disclosure so that JCPS may seek a protective order or other appropriate remedy to prevent the disclosure or to ensure JCPS's compliance with the confidentiality requirements of federal or state law; provided, however, that Services Provider will use all reasonable efforts to maintain the confidentiality of confidential and otherwise

personally identifiable data. If a protective order or other remedy is not obtained prior to the deadline by which any legally compelled disclosure is required, Services Provider will only disclose that portion of confidential and otherwise personally identifiable data that Services Provider is legally required to disclose.

4. Services Provider shall not distribute, reprint, alter, sell, assign, edit, modify or create derivative works or any ancillary materials from or with the data.
5. Services Provider shall not use data shared under this Agreement for any purpose other than the services contract described in Paragraph B.1 above. Nothing in this Agreement shall be construed to authorize Services Provider to have access to additional data from JCPS that is not included in the scope of this Agreement (or addenda). Services Provider understands that this Agreement does not convey ownership of the data to Services Provider.
6. Services Provider shall take reasonable security precautions and protections to ensure that persons not authorized to view the data do not gain access to the data. Reasonable security precautions and protections include, but are not limited to:
 - a. Creating, distributing, and implementing data governance policies and procedures which protect data through appropriate administrative, technical and physical security safeguards, and outline staff responsibilities for maintaining data security;
 - b. Encrypting all data carried on mobile computers/devices;
 - c. Encrypting data before it is transmitted electronically;
 - d. Requiring that users be uniquely identified and authenticated before accessing data;
 - e. Establishing and enforcing well-defined data privilege rights which restrict users' access to the data necessary for this to perform their job functions;
 - f. Ensuring that all staff accessing data sign a nondisclosure statement, attached as **Attachment B**, and maintain copies of signed statements;
 - g. Securing access to any physical areas/electronic devices where sensitive data are stored;
 - h. Installing a firewall to permit or deny network transmissions based upon a set of rules; and
 - i. Installing anti-virus software to protect the network.

7. If Services Provider receives Personal Information as defined by and in accordance with the Kentucky Personal Information Security and Breach Investigation Procedures and Practices Act, KRS 61.931, et seq. (the "Act"), Services Provider shall secure, protect and maintain the confidentiality of the Personal Information by, without limitation, complying with all requirements applicable to "non-affiliated third parties" set forth in the Act, including but not limited to the following:
- a. "Personal Information" is defined in accordance with KRS 61.931(6) as an individual's first name or first initial and last name; personal mark; or unique biometric or genetic print or image, in combination with one (1) or more of the following data elements:
 - i. An account, credit card number, or debit card number that, in combination with any required security code, access code or password, would permit access to an account;
 - ii. A Social Security number;
 - iii. A taxpayer identification number that incorporates a Social Security number;
 - iv. A driver's license number, state identification card number or other individual identification number issued by an agency;
 - v. A passport number or other identification number issued by the United States government; or
 - vi. Individually Identifiable Information as defined in 45 C.F.R. sec. 160.013 (of the Health Insurance Portability and Accountability Act), except for education records covered by FERPA.
 - b. As provided in KRS 61.931(5), a "non-affiliated third party" means any person or entity that has a contract or agreement with an agency and receives (accesses, collects or maintains) personal information from the agency pursuant to the contract or agreement.
 - c. Services Provider shall not re-disclose, without the written consent of JCPS, any "personal information," as defined in KRS 61.931, or any other personally identifiable information of a student or other persons, such as employees.
 - d. Services Provider agrees to cooperate with JCPS in complying with the response, mitigation, correction, investigation, and notification requirements of the Act.

- e. Services Provider agrees to undertake a prompt and reasonable investigation of any breach as required by KRS 61.933.
8. If Services Provider is a cloud computing service provider (as defined in KRS 365.734(1)(b) as "any person other than an educational institution that operates a cloud computing service"), Services Provider agrees that:
- a. Services Provider shall not process student data for any purpose other than providing, improving, developing, or maintaining the integrity of its cloud computing services, unless the provider receives express permission from the student's parent. Services Provider shall work with the student's school and district to determine the best method of collecting parental permission. KRS 365.734 defines "process" and "student data."
 - b. Pursuant to KRS 365.734(2), Services Provider shall not in any case process student data to advertise or facilitate advertising or to create or correct an individual or household profile for any advertisement purposes.
 - c. Pursuant to KRS 365.734(2), Services Provider shall not sell, disclose, or otherwise process student data for any commercial purpose.
 - d. Pursuant to KRS 365.734(3), Services Provider shall certify in writing to the agency that it will comply with KRS 365.734(2).
9. Services Provider shall report all known or suspected breaches of the data, in any format, to Dr. Kermit Belcher, Chief Information Officer. The report shall include (1) the name, job title, and contact information of the person reporting the incident; (2) the name, job title, and contact information of the person who discovered the incident; (3) the date and time the incident was discovered; (4) the nature of the incident (e.g. system level electronic breach, an electronic breach of one computer or device, a breach of hard copies of records, etc.); (5) a description of the information lost or compromised; (6) the name of the electronic system and possible interconnectivity with other systems; (7) the storage medium from which information was lost or compromised; (8) the controls in place to prevent unauthorized use of the lost or compromised information; (9) the number of individuals potentially affected; and (10) whether law enforcement was contacted.
10. Services Provider shall securely and permanently destroy the data, and any and all hard and soft (electronic) copies thereof, upon the termination of this Agreement. Services Provider agrees to require all employees, contactors, or agents of any kind using JCPS data to comply with this provision. Services Provider agrees to document the methods used to destroy the data, and upon request, provide certification to JCPS that the data has been destroyed.
11. For purposes of this agreement and ensuring Services Provider's compliance with the terms of this Agreement and all application of the state and Federal laws, Services Provider designates Glenn Adams its Chief Product Officer (or an

alternative designee specified in writing) as the temporary custodian ("Temporary Custodian") of the data that JCPS shares with Services Provider. JCPS will release all data and information under this Agreement to Temporary Custodian. Temporary Custodian shall be responsible for transmitting all data requests and maintain a log or other record of all data requested and received pursuant to this Agreement, including confirmation of the return or destruction of the data as described below. JCPS or its agents may, upon request, review the records Services Provider is required to keep under this Agreement.

12. Services Provider acknowledges that any violation of this Agreement and/or the provisions of FERPA or accompanying regulations related to the nondisclosure of protected student information constitutes just cause for JCPS to immediately terminate this Agreement.
13. Services Provider shall maintain, during the term of this Agreement, a cyber-insurance liability policy, in the amount of \$5M. Upon request, Services Provider shall furnish the certificate of insurance evidencing this coverage. The certificate of insurance shall name the Board of Education of Jefferson County as additional insured in the Description of Operations section of the Certificate of Insurance which shall read:

Board of Education of Jefferson County
Attn: Insurance/Real Estate Dept.
3332 Newburg Road
Louisville, Kentucky 40218

14. Services provider shall maintain, during the term of this Agreement, ISO27001 or SOC2 certification. If Services Provider is unable to provide ISO27001 or SOC2 certification, minimum requirements on a JCPS-provided standardized questionnaire must be met. Upon request, Services Provider shall furnish a current ISO27001, SOC2 certification, or updated questionnaire.

E. FINANCIAL COSTS OF DATA-SHARING

Each party shall be responsible for their portion of costs that may result from data sharing. Examples of potential costs to JCPS are costs associated with the compiling of student data requested under this agreement and costs associated with the electronic delivery of the student data to Services Provider.

No payments will be made under this Agreement by either party. Any payments to Services Provider will be made under the services contract described in Paragraph B.1 above.

F. OBLIGATIONS OF JCPS

During the term of this Agreement, JCPS shall:

1. Prepare and deliver the data described in **Attachment A**.

G. LIABILITY

Services Provider agrees to be responsible for and assumes all liability for any claims, costs, damages or expenses (including reasonable attorneys' fees) that may arise from or relate to Services Provider's intentional or negligent release of personally identifiable student, parent or staff data ("Claim" or "Claims"). Services Provider agrees to hold harmless JCPS and pay any costs incurred by JCPS in connection with any Claim. The provisions of this Section shall survive the termination or expiration of this Agreement.

H. TERMINATION

1. This Agreement may be terminated as follows, after notification via the United States Postal Service (certified mail or registered mail) or recognized overnight delivery service (e.g., UPS, DHL, or FedEx):
 - a. By either party in the event of a material breach of this Agreement by another party provided however, the breaching party shall have thirty (30) days to cure such breach and this Agreement shall remain in force.
 - b. By either party after thirty (30) days advance written notice to the other party, for any reason or no reason.
2. The confidentiality provisions of this Agreement shall survive the termination of this Agreement. If this Agreement is terminated by either party for material breach or for any other reason with thirty (30) days written notice, within seven (7) days of the termination the confidential information shall be returned or destroyed within seven (7) days of the termination and the Temporary Custodian shall provide JCPS confirmation of the return or destruction of the data pursuant to Paragraph D.11. If this Agreement terminates at the end of the term described in Section A, within seven (7) days after the end of the term, Services Provider shall return or destroy all confidential information and the Temporary Custodian shall provide JCPS confirmation of the return or destruction of the data pursuant to Paragraph D.11.
3. Destruction of the confidential information shall be accomplished by utilizing an approved method of confidential destruction, including but not limited to shredding, burning or certified/witnessed destruction for physical materials and verified erasure of magnetic media using approved methods of electronic file destruction.

I. PUBLICATIONS AND COPYRIGHTS

Both parties recognize that each organization may have extant work that predates this agreement. If those materials and/or data are used in the course of this work, they remain the property of the original developer. If new materials are developed during the term of the services contract described in Paragraph B.1 above, ownership and copyright of such will be governed by the terms of the services contract.

Any notices or reports by one party to the other party under this Agreement shall be made in writing, to the address shown in the signature portions of this Agreement, or to such other address as may be designated in writing by one party to the other. Notices shall be effective when received if personally delivered, or three days after mailing if mailed.

Q. RELATIONSHIP OF PARTIES


JCPS is not an employee, agent, partner or co-venturer of or with Services Provider. Neither Services Provider nor JCPS shall represent or imply to any party that it has the power or authority to enter into a contract or commitment in the name of or on behalf of the other, or to otherwise bind the other.

R. ENTIRE AGREEMENT; ASSIGNMENT

This Agreement, together with any attachments hereto and any amendment or modifications that may hereafter be agreed to, constitute the entire understanding between the parties with respect to the subject-matter hereof and supersede any and all prior understandings and agreements, oral and written, relating hereto. Services Provider shall not assign this Agreement or any portion thereof to a subcontractor or other third party without the prior written consent of JCPS, and any attempted assignment without such prior written consent in violation of this Section R shall automatically terminate this Agreement.

AGREED:

SoftChalk LLC/o 2441 Nacogdoches Road, PMB 535
San Antonio, TX 78217

BY: 

Name: Cristina Wheless

Title: General Manager

Date: April 19, 2022

AGREED:

Jefferson County Board of Education
3332 Newburg Road
Louisville KY 40218

BY: _____

Name: Martin A. Pollio, Ed. D.,

Title: Superintendent

Date: _____

Attachment A (Of the Data Sharing Agreement)

CONFIDENTIAL INFORMATION TO BE DISCLOSED

Please list each individual data field, not generic categories, we will share with you based off your API specifications or data file import layout – no fields should be designated as optional

Student First Name

Student Last Name

4.19.2022 - G/DRIVE

ATTACHMENT B



Volaris Group Corporate Policies

VOLARIS GROUP CODE OF CONDUCT

Volaris Group Inc. (the “**Company**” or “**Volaris Group**”) is committed to conducting business in a professional and ethical manner. This Code of Conduct (the “**Code**”) will apply to all directors, officers and employees (collectively the “**Representatives**” and individually a “**Representative**”) of Volaris Group Inc. and each of its direct and indirect subsidiaries (collectively such entities referred to as the “**Company**”). This Code will be periodically reviewed to capture changes in the law, reputational demands and changes in the Company’s business and geographical reach.

1. General Purpose. The purpose of this Code is to promote honest and ethical conduct. It is intended to be a general guide and not a comprehensive rulebook. This Code may reinforce or supplement various policies of the Company that are already in place or which may be adopted. This Code is intended to be observed in conjunction with such policies and procedures. This code shall also be read and interpreted in conjunction with applicable local laws, which may include more restrictive obligations (in which case, the more restrictive obligation will apply). In the event of any question or concern with respect to how this Code applies, any Representative should consult with their his/her immediate supervisor or with the General Counsel or Chief Financial Officer of Volaris Group.

2. Compliance with Law

2.1 General. All business affairs of the Company must be conducted in compliance with all applicable laws, rules and regulations and in accordance with the highest standards of honesty, integrity and ethical behavior, in all the jurisdictions in which the Company does business. Representatives are expected to use good judgment and common sense in seeking to ensure compliance with applicable law, and to seek advice from his or her supervisor if uncertain as to the proper course of action. If a Representative becomes aware of the violation of any law, rule or regulation by the Company, whether by its officers, employees, directors, or any third-party doing business on behalf of the Company, he or she must promptly report the matter as set out in Section 6 of this Code.

2.2 Financial Reporting. The Company’s financial statements and all books and records on which they are based must be materially complete and accurate so that they reflect the state of the Company’s business. This requirement applies regardless of whether such records would disclose disappointing results or a failure to meet anticipated profit levels. Any attempt to mask actual results by inaccurately reflecting costs or sales will not be tolerated. If a Representative has concerns or complaints regarding questionable accounting or auditing practices of the Company, including a failure to comply with internal controls of the Company or to cooperate with the Company’s internal or independent auditors, he or she should report those concerns or complaints in accordance with Section 6 of this Code.

2.3 Insider Trading. As an operating group of Constellation Software Inc., a company publicly traded on the Toronto Stock Exchange, the Company is subject to applicable securities laws and regulations. As a part of their work for the Company, Representatives may acquire inside or non-public



information about the Company or its affiliates, or about other companies with which there may be pending or proposed transactions. Securities laws prohibit persons having material inside information from disclosing such information or from purchasing, selling or otherwise trading in the securities of such companies until after the information has been published to the general public. These laws prohibit selling securities while in possession of unfavorable inside information to avoid losses and purchasing securities while possessing favorable inside information to obtain profits. Violation of these laws can result in civil penalties, criminal fines or imprisonment.

Prior to full public disclosure, Representatives must not discuss or make public important business developments involving the Company, any subsidiary or any other relevant entity, in even the most casual manner, with family, friends, outsiders or other employees who do not need to have such information. Giving a “tip” to someone else based on inside information is illegal. Both the discloser and the person given the “tip” may be subject to significant criminal and civil penalties if securities are traded based on a disclosure of inside information. Representatives should review the attached Constellation Software Inc. Summary of Disclosure, Confidentiality & Insider Trading Policy if in any doubt as to the applicability of the foregoing standards.

2.4 Protection of Personal Information. Representatives are expected to act in compliance with all applicable privacy laws and should only acquire or retain personal information in the course of their work where it is required by law, requested by customers or required in connection with the operation of the Company’s business. Access to any such personal information is to be restricted internally to those with a legitimate need to know and Representatives must not market, sell or otherwise disclose such personal information in any manner whatsoever. Employee communications transmitted through or by the Company’s computer systems are not considered to be private and may be monitored or restricted by authorized Company personnel.

2.5 Anti-Bribery and Anti-Corruption. The Company takes a zero-tolerance approach to bribery and corruption in all the jurisdictions in which the Company does business and is committed to implementing and enforcing effective systems to counter bribery and corruption. Bribery is offering, promising, providing or receiving something of value (such as cash, gifts or hospitality) as an inducement or reward in order to gain any commercial, contractual, or personal advantage.

Representatives (or someone on their behalf, or a family member thereof) must not:

- a. give, promise to give, or offer, a payment, gift or hospitality with the expectation or hope that a business advantage will be received, or to reward a business advantage already given;
- b. give, promise to give, or offer, a payment, gift or hospitality to a government official, agent or representative to "facilitate" or expedite a routine procedure;
- c. accept payment from a third party that you know or suspect is offered with the expectation that it will create a business advantage for them;
- d. accept a gift or hospitality from a third party if you know or suspect that it is offered or provided with an expectation that a business advantage will be provided in return; or
- e. threaten or retaliate against another worker who has refused to commit a bribery offence or who has raised concerns under this Code.



The Company does not prohibit reasonable, proportionate and appropriate gifts or hospitality given to or received from third parties, provided it is in accordance with this Code. Bona fide hospitality and promotional or other business expenditure which seeks to improve the image of the Company, to present the Company's products and services, or to establish cordial relations, is recognized as an established and important part of doing business. However, the recipient of any gift and/or hospitality should not be given the impression that he/she is under an obligation to confer any business as a result of the hospitality itself, or that his/her independence will be affected by receiving any such hospitality.

Representatives must consider whether in all the circumstances the gift or hospitality is reasonable, proportionate and appropriate, including the following considerations:

- a. what the intention of the gift or hospitality is;
- b. whether there is any secrecy involved;
- c. the value of the gift/hospitality (the higher the value, the less likely it is to be appropriate); and
- d. how the gift or hospitality would reflect on the Company if the details were made public.

Circumstances that are usually acceptable include:

- a. occasional lunches and dinners with existing and prospective customers and suppliers;
- b. occasional attendance at sports, theatre and other cultural events; and
- c. gifts of nominal value or other small promotional items.

Circumstances which would usually not be appropriate include:

- a. gifts of cash or a cash equivalent;
- b. gifts in your name, not in the Company's name;
- c. secret gifts; and
- d. any gifts given to or received from suppliers, government officials or representatives to obtain or retain an improper advantage.

3. Conflicts of Interest. Representatives must act in the best interests of the Company in all circumstances and are not permitted to engage in any activity that conflicts with the interests of the Company. A conflict of interest exists whenever a Representative's private interests interfere or appear to interfere with the Company's interests and may arise whenever a Representative takes action or has an interest that prevents that person or appears to prevent that person from performing their duties for the Company openly, honestly, objectively, and effectively. Some common examples of conflicts of interest are:

- a. Having a financial interest in a company that competes with or does business with the Company;
- b. Holding a position as a director, officer, employee or consultant of an enterprise that competes with or does business with the Company;
- c. Acceptance by a Representative (or a family member thereof) of any gifts or hospitality other than in accordance with Section 2.5 of this Code;
- d. Taking personal advantage of an opportunity in which the Company has an interest;



- e. Diverting a business opportunity from the Company for personal benefit or using position within the Company to influence the Company to do business with or give preferential treatment to a friend or relative (or a company with which the friend or relative is associated in a significant role); and
- f. Using Company funds, facilities, personnel or other assets for personal benefit.

If a Representative, directly or indirectly, enters into an activity or obtains an interest (or if one already exists) that appears to contravene any of the above, that person must disclose the fact relating to the activity or interest in writing to the Company's Chief Financial Officer or General Counsel, and such Representative will be required to take whatever action is determined by the Company to be appropriate to cure any conflict which is found to exist.

4. Use of Company Property. Representatives must use best efforts to protect the assets of the Company, including facilities, computer equipment, and any other physical property, from unauthorized use, loss, theft or misuse. All Company assets should be used for legitimate business purposes only and not for personal benefit. The use of any Company funds or assets for any unlawful or improper purpose is strictly prohibited. Claims for travel and entertainment expenses must be fair and relate only to Company business. Credit cards issued for travel and other Company business are not to be used for personal purposes.

5. Fair Competition. The Company seeks to build lasting relationships with customers and business partners, and to outperform its competition, in a fair and honest manner. The Company's policy is to compete with fairness and integrity in all the markets in which it participates. Representatives must always deal fairly with the Company's shareholders, customers, suppliers, competitors and employees. Representatives must not give gifts, gratuities, favors or benefits to any government officials or to any third parties if such items are beyond what could reasonably be considered ethical and within accepted business practices. Representatives must not take unfair advantage of others through manipulation, concealment, and abuse of privileged information, misrepresentation or any other intentionally unfair dealing.

6. Reporting Violations of the Code. Every Representative has an obligation to be familiar with the terms of this Code, and to ask questions, seek guidance and express any concerns with respect to its terms. Any person who has knowledge of a potential, suspected, or known violation of this Code has an obligation to report this information to his or her manager, or alternatively to the Chief Financial Officer or General Counsel of the Company. If requested, the Company will attempt to handle such concerns or complaints confidentially, subject to the requirements of applicable law. The Company will not permit retaliation of any kind by or on behalf of the Company or its directors, officers or employees against good faith reports of violations of this Code or any other illegal or unethical conduct.

7. Disciplinary Action. The Company intends to enforce the provisions of this Code. Any violation of the Code, including a failure to report a violation, or retaliation against another employee who, in good faith, reports a violation, may lead to disciplinary action being taken, up to and including dismissal for cause. Although any Representative who discloses his or her own misconduct may be subject to disciplinary action, the Company may consider such voluntary self-disclosure as a mitigating factor.



CONSTELLATION SOFTWARE INC.

SUMMARY OF DISCLOSURE, CONFIDENTIALITY & INSIDER TRADING POLICY

1. **Purpose of this Policy.** Ensure: that Constellation Software Inc. (TSX: CSU) (the Corporation) complies with its timely disclosure; that all disclosures are accurate and complete; that documents released by the Corporation or public oral statements do not contain misrepresentations; that all persons understand their obligations to preserve the confidentiality of Undisclosed Material Information; and that all parties who have Undisclosed Material Information understand that they are prohibited from Insider Trading or Tipping.

2. **To Whom this Policy Applies.** Board Members, Officers, Employees and Contractors, and any spouse, live-in partner or relative of any of these individuals who resides in the same household as that individual.

3. **Responsibility for this Policy.** The Corporation has a corporate disclosure committee responsible for overseeing the Corporation's disclosure practices under this Policy, which will consist of the Chief Financial Officer ("CFO"), the President of the Corporation and the Secretary of the Corporation.

It is essential that the Disclosure Committee be kept fully apprised of all pending material developments of the Corporation in order to evaluate and discuss those events and to determine the appropriateness and timing for public release of information.

4. **Individuals Who Are Authorized to Speak on Behalf of the Corporation.** Only the individuals listed below are authorized to communicate with analysts, the media and investors on behalf of the Corporation and only with respect to the areas noted opposite their respective names.

<u>Spokesperson</u>	<u>Area</u>
President	All areas
CFO	All areas
COO	All areas
VP, Business Development	All areas

Other than as set out above, approval from either the President or CFO is required prior to any communication with analysts, media or investors on behalf of the Corporation.



5. **Timely Disclosure of Material Information.** “Material information” means a fact or change that would reasonably be expected to have a significant effect on the market price or value of the securities of the Corporation.

If the event constitutes a material change, prepare a press release and a material change report describing the material change as required under applicable laws.

6. **Internet Chat Rooms and Bulletin Boards.** Do not discuss or post any information relating to the Corporation or any of its subsidiaries or trading in securities of the Corporation in Internet chat rooms, newsgroups, bulletin boards, web logs or other electronic media available to the public.

7. **Rumors.** The Corporation shall not comment, affirmatively or negatively, on rumors.

8. **Quiet Period.** Each period (a) beginning on the last day of each fiscal quarter and each fiscal year, and (b) ending when the earnings for that quarter or year have been Generally Disclosed by way of a news release, will be a “Quiet Period”. During a Quiet Period, Spokespersons won’t talk to any outsider.

9. **Avoiding Selective Disclosure.** A shareholder meeting or analyst meeting does not qualify as “General Disclosure”, hence no new material facts/changes may be disclosed there.

10. **Analyst Reports.** Any comments must contain a disclaimer that the report was reviewed **for factual accuracy only**... and that only Generally Disclosed information can be reviewed. Analysts' reports must not be circulated by the company.

11. **Trading of Securities of the Corporation.** Board Members, Officers, Employees and Contractors shall not purchase or sell or otherwise monetize securities of the Corporation except during a “Trading Window”. “Trading Window” means 3 trading days after the financial results have been disclosed by way of a news release, and end on the 14th day of the last month of that quarter.

12. **Insider Trade Reports.** An Insider of the Corporation is required to file an initial insider report through SEDI, within ten (10) days of becoming an Insider and subsequent insider reports within five (5) calendar days following any trade of securities of the Corporation.



VOLARIS INFORMATION TECHNOLOGY POLICY

Henceforth, “**The Company**” or “**Company**” will represent Volaris Group Inc., and any subsidiary legal entities, companies, business units or brands.

All users (“**Users**”) of the computers and related systems (collectively, the “**Computers**”) of the Company and the Company’s internal networks, connection to the Internet and online services (collectively, the “**Networks**”), including employees, consultants and independent contingent workers performing services for the Company, are to comply with the following rules. Violations of these rules are grounds for disciplinary action, including dismissal, and may also subject the user to penalties or proceedings under civil law, copyright law or criminal law.

- 1. Confidential Information.** You are likely, during the course of your employment, to come into the possession of information relating to the business of the Company or of our customers. Be aware that such information is to be treated as confidential irrespective of its content. This duty of confidence remains if you leave the Company.

Knowledge relating to Customer and Supplier information or corporately sensitive information about Customer requirements is to be regarded as ‘Commercial in Confidence’.

Irrespective of formal data classification schemes, Commercial in Confidence data can be identified as information that, if disclosed, may result in damage to a party's commercial interests, intellectual property or trade secrets.

Sensitive data could encompass a wide range of information and can also include: ethical or racial origin, political opinion, religious or similar beliefs, union memberships, physical or mental health details.

All employees have a duty of care where confidential information is concerned. Such information should not be reproduced (such as electronic copies or photocopies) unless necessary and should never be sent or given to anyone who is not an employee without first obtaining permission in writing from the Company.

- 2. Disclosure of Information.** You are not to directly or indirectly disclose to any unauthorised person any knowledge or information relating to the Company’s business, or the business of any of the Company’s employees or customers without first obtaining permission in writing from the Company.

You must not use for your own purposes or profit or for any purposes other than those of the Company, any information which you may acquire in relation to the Company’s and/or its customers’ business

No employee is to disclose any confidential information, either while employed or after having left the organisation, except in the proper course of your employment or unless required to do so by law.

If you are required to do so by law, you must inform your line manager and provide them with information about work-related content/data that may have been accessed. Managers are to use their discretion to



determine if further escalation is required to their business leader, based on the sensitivity and type of data accessed. Especially for client data, there may be additional regulatory compliance to consider.

3. Data Security. The Company may adopt additional operational policies to ensure the confidentiality, integrity and availability of its customer's and company and/or employee data, and may periodically update these policies. These will be stored on the Company Intranet, and when updated employees will be advised accordingly.

Customer data, where practicable, should reside within the corporate boundary and only stored in appropriate locations. In circumstances whereby copies of customer data is stored locally on your hard drive you should ensure that your hard drive has been encrypted to the Company standard. Further information may be obtained from the Company IT department.

4. Data Protection. For various reason (operating in new geographies for example), the Company may from time to time, be required to comply with particular Data Protection policies. The Company considers that compliance with these policies is of paramount importance and will provide information and training to all employees as appropriate to their role and responsibilities as necessary. Adherence to these Data Protection policies takes precedent over guidelines. Guidelines are available on the Intranet.

Any suspected or actual Data Protection breach must be reported immediately. Appropriate procedures may be found on the Company Intranet. A wilful breach of Data Protection will be considered as gross misconduct and will result in disciplinary action up to and including termination.

5. Use of Company Equipment. The Company should provide employees with the necessary tools to carry out their daily duties. All items remain the property of the Company, but the user (employee) is to ensure that the equipment is well maintained and adequate precautions are taken to ensure that all items remain secure even when it is not in use. All electronic items (i.e. laptops, mobile phones, tablets etc.) are not be left or stored in vehicles or unsecured locations.

All losses or damage to any item should immediately be reported to both your Line Manager and the Company IT department.

The Company reserves the right at a point in time to engage in a Bring Your Own Device/Computer (BYOD/BYOC) or similar program(me).

If the lost device holds sensitive personal data (Company or Customer) this should be reported to your line manager, HR and Data Security immediately.

6. Software. The Company may adopt additional Software use policies to help define/clarify authorised Software copies.

Software (Commercial or otherwise) either downloaded over the Internet or available on media, should not be installed on any of the Company's computers or the Company's supported customer's computers without prior approval of the Company IT department or it's delegates. Where approval is obtained, software should only be installed in line with appropriate licensing agreements and applicable installation procedures.



The Company IT department may inspect computers periodically to verify that only approved and/or licensed software has been installed and may without prior warning, remove any unlicensed or illegal software.

6. Anti-Virus / Anti-Malware. A virus or malware is a piece of potentially malicious programming code that could cause some unexpected or undesirable event. These can be transmitted electronically, usually via email or instant messaging attachments, downloadable Internet files, diskettes, and CDs. A virus infection can be very costly to any business in terms of lost data, lost staff productivity, and/or lost reputation.

To limit these effects, the Company implements Anti-virus and/or Anti-malware software.

Any security enhancement that exists on any Company computer is not be modified or disabled without prior consent of the Company IT department.

You are not to connect any unauthorised PC, laptop, server or any other hardware device directly to any of the Company's supported customer networks or the Company networks. Additionally, you must not make any changes to the Company's cabling infrastructure used for local area networks and telephony.

7. Passwords. Passwords are an important component of information and network security. The use of a user ID and password combination serves to identify and authenticate a user to system resources and information assets. It is only through authenticated access that the enterprise can be assured that systems and data are being used appropriately.

As such, passwords are to be constructed, used and protected appropriately to ensure that the level of security they imply is actually met.

- a. Passwords should not be based on well-known or easily accessible information, including personal information.
- b. Passwords should not be words commonly found within a standard dictionary, unless used as a consecutive passphrase (for example, MaryHad2LittleLamb5!).
- c. Users will be notified 15 Days in advance of password expiration. At that point, and at defined subsequent days until a change is made, users will be prompted to select a new password.
- d. The Company uses technical measures to ensure that users conform to the policy.
- e. Upon termination of role, any and all passwords or access codes are to be divulged to the Company.

8. Monitoring and Auditing. Monitoring and auditing is used to determine if inappropriate actions, either intentional or accidental, have occurred within an information system.

System Monitoring forms the basis of IT Operations checks. These include but are not limited to system integrity, system health and availability or uptime.

Auditing provides the basis of establishing an identity associated with a process within any given system.

The Company reserves the absolute right to monitor and/or audit an employees' use of systems, including but not limited to e-mail and internet activity occurring on or via Company equipment or accounts, and may employ filtering software (for example, to limit access to sites on the Internet).



If the Company discovers activities which do not comply with applicable law or departmental policy, records retrieved may be used to document the wrongful content in accordance with due process.

9. Acceptable / Unacceptable Use.

- a. Appropriate use examples: Individuals are encouraged to use email and the Internet to further the goals and objectives of the business. The types of activities that are encouraged include:
 - i. Communicating with fellow employees, business partners, and clients within the context of an individual's assigned responsibilities;
 - ii. Acquiring or sharing information necessary or related to the performance of an individual's assigned responsibilities; and
 - iii. Participating in educational or professional development activities.

Specific guidance on social media can be found on the Company Intranet

- b. Inappropriate use examples: Individual email or Internet use will not interfere with others' productive use of Company resources. Users will not violate the network policies of any network accessed through their account. Internet use will comply with all Country specific, Federal and State/Provincial laws, all Company policies and contracts. This includes, but is not limited to, the following:
 - a. The Internet may not be used for illegal or unlawful purposes, including, but not limited to, copyright infringement, obscenity, libel, slander, fraud, defamation, plagiarism, harassment, intimidation, forgery, impersonation, illegal gambling, soliciting for illegal pyramid schemes, and computer tampering (e.g. spreading computer viruses).
 - b. The Internet may not be used in any way that violates the Company's policies, rules, or administrative orders including, but not limited to, the Company code of conduct.
 - c. Use of the Internet in a manner that is not consistent with the mission of the Company, misrepresents the Company, or violates any Company policy is prohibited.
 - d. The Company prohibits use for mass unsolicited mailings, access for non-employees to the Company resources or network facilities, uploading and downloading of files for personal use, access to pornographic sites, gaming, competitive commercial activity unless pre-approved by the Company, and the dissemination of chain letters.
 - e. Individuals may not establish company computers as participants in any peer-to-peer network, unless approved by management.
 - f. Individuals may not view, copy, alter, or destroy data, software, documentation, or data communications belonging to the Company or another individual without authorized permission.
 - g. Use of non-approved / Company provided services, such as non-commercial instant messaging or voice communication over the Internet.



- h. Use of email for illegal or unlawful purposes, including copyright infringement, obscenity, libel, slander, fraud, defamation, plagiarism, harassment, intimidation, forgery, impersonation, soliciting for illegal pyramid schemes, and computer tampering (e.g. spreading of computer viruses).
- i. Use of email in any way that violates the Company policies, rules, or administrative orders, including, but not limited to, the Company code of conduct.
- j. Viewing, copying, altering, or deletion of email accounts or files belonging to the Company or another individual without authorized permission.
- k. Sending of unreasonably large email attachments. The total size of an individual email message sent (including attachment) should be 35MB or less.
- l. Opening email attachments from unknown or unsigned sources. Attachments are the primary source of computer viruses and should be treated with utmost caution.
- m. Sharing email account passwords with another person or attempting to obtain another person's email account password. Email accounts are only to be used by the registered/authorized user.
- n. Excessive personal use of the Company email resources. The Company allows limited personal use for communication with family and friends, independent learning, and public service so long as it does not interfere with staff productivity, pre-empt any business activity, or consume more than a trivial amount of resources.
- o. The Company prohibits personal use of its email systems and services for unsolicited mass mailings, non-company commercial activity, political campaigning, dissemination of chain letters, and use by non-employees.



VOLARIS SOCIAL MEDIA POLICY

1. **Scope/Purpose of this document.** This document reflects the current guidelines as determined by the Company in collaboration with employees. This document is subject to modifications and amendments from time to time as required.

Volaris and its subsidiaries would like to encourage the use of Social Media by employees, customers, partners and others as it can be a valuable way to stimulate discussion, demonstrate transparency and share information regarding our company and our products.

Henceforth, “The Company” or “Company” will represent either Volaris Group Inc., and any subsidiary legal entities, companies, business units or brands.

The Volaris Social Media Policy applies to:

- a. All blogs, wikis, forums, and social networks hosted or sponsored by the Company
- b. Your personal blogs that contain postings about The Company’s business, products, employees, customers, partners, or competitors
- c. Your postings about The Company’s business, products, employees, customers, partners, or competitors on external blogs, wikis, discussion forums, or social networking sites such as LinkedIn, Twitter and Facebook
- d. Your participation in any audio or video related to The Company’s business, products, employees, customers, partners, or competitors, whether you create a video to post or link to on your blog, you contribute content for a video, or you appear in a video created either by another employee or by a third party.

Even if your Social Media activities take place completely outside of work, what you say can have an influence on your ability to conduct your job responsibilities, those of your teammates, those of The Company and its business interests.

Employees at The Company are expected to act with integrity and diligence at all times during their employment. They are also bound by The Company’s policies and guidelines, which govern their conduct. These require that employees exercise honesty in all business dealings relating to their employment. Failure to do so will result in discipline, up to and including termination of employment, and may result in prosecution of the employee by legal authorities. Employees are subject to discipline up to and including termination of employment for other inappropriate actions and inactions not referenced in the this policy. Please refer to the **Volaris Group Code of Conduct**.

2. **Social Media Center of Excellence (SMCE).** This centralized group provides services to business units and its purpose is to set guidelines, branding, policies and processes, provide education and training, while reducing or eliminating risk. The SMCE will administer all tools, distribute best practices and keep publishers/contributors informed of any changes, news or trends. Business units will be responsible for



their own content and have a champion(s) that will engage customers and/or employees according to this and other policies developed by the SMCE or The Company.

Training classes will be available for employees wanting to use Social Media on their own and those who are engaging customers and employees on behalf of The Company. The SMCE will develop and record Webcasts and publish news, trends and useful information on the SMCE blog found on The Company Intranet.

All contributors will meet periodically with the SMCE to discuss strategy, tools, concerns and share relevant information related to Social Media at The Company.

3. **Guiding Principles for All Employees.** There's a big difference in speaking "on behalf of the Company" and speaking "about" The Company. This set of principles refers to those personal or unofficial online activities where you might refer to The Company.

a. Adhere to the Code of Business Conduct and other applicable policies.

- I. All employees and contractors are subject to the Code of Conduct and all policies, including the Media Policy, Disclosure, Confidentiality and Insider Trading Policy and Information Systems Policy. These policies are applicable to your business and personal activities online.
- II. You must not comment publicly on The Company's M&A activity, including potential and pending acquisitions. This applies to potential acquisitions regardless of their status - in diligence, announced but not closed, etc.
- III. Don't discuss product upgrades, new features or future product releases. Please note that any direct communication to analysts, the financial market and/or members of the media must be conducted only by official Company representatives

b. We encourage you to review your Employee Handbook if you have any questions about this policy. You may also contact your HR representative if you have any further questions. **You are responsible for your actions. Anything you post that can potentially tarnish the Company's image will ultimately be your responsibility. We do encourage you to participate in the online Social Media space, but urge you to do so properly, exercising sound judgment and common sense. If you feel you might have violated this purposely or in error, please email social.media@volarisgroup.com.**

c. Be a "scout" for compliments and criticism. Even if you are not an official online spokesperson for the Company, you are one of our most vital assets for monitoring the Social Media landscape. If you come across positive or negative remarks about the Company or its brands online that you believe are important, consider sharing them by forwarding them to social.media@volarisgroup.com.

d. Let the subject matter experts respond to negative posts. You may come across negative or disparaging posts about the Company or its brands, or see third parties trying to spark negative conversations. Unless you are a certified online spokesperson, avoid the temptation to react



yourself. Pass the post(s) along to our official in-market spokespersons that are trained to address such comments at social.media@volarisgroup.com

- e. **Be conscious when mixing your business and personal lives.** Online, your personal and business personas are likely to intersect. The Company respects the free speech rights of all of its associates, but you must remember that customers, colleagues and supervisors often have access to the online content you post. Keep this in mind when publishing information online that can be seen by more than friends and family, and know that information originally intended just for friends and family can be forwarded on. Remember NEVER to disclose non-public information of the Company (including confidential information), and be aware that taking public positions online that are counter to the Company's interests might cause conflict.

4. **Personal Spaces on the Web.** You are free to set up any blog, space or other area within the given framework of the terms provided by the host of such spaces (e.g. Facebook, LinkedIn, Twitter, etc). The SMCE will help you if you need assistance with setting up a Social Media channel if you have any questions. Please email social.media@volarisgroup.com whenever you intend to use The Company any part of the name or URL to obtain permission and avoid confusion with communication from The Company. Do not post inappropriate, disrespectful comments to your blog, or post comments that are intended to embarrass The Company, your co-workers, customers, partners or competitors. Any personal space where you identify yourself and could be associated or identified with The Company in any way should have a clear disclaimer that it is not an official space of The Company. This policy is to protect both the employee and the company. The following basic template may be used for this purpose:

"The opinions on this Web site/blog/other are those of the author and do not represent the views, express or implied, of any past or present employer and/or organization."

If you need any help with drafting a notice, please email social.media@volarisgroup.com.

This policy is to protect both the employee and the Company.

Please do not use a personal account to conduct company business, nor use a company account for personal business.

It is important not to post Company content on public Web sites or Social Media spaces including photos, videos or company collateral. Please refrain from posting personal photos or information of employees from Company events that could harm The Company, employees or anyone associated with The Company.

Managers and their subordinates are free to "friend" each other on social networking sites. Both managers and employees, however, should be mindful of avoiding any interactions/communications that may create a conflict of interest or that may compromise The Company's ability to enforce its policies, especially its policies against nepotism, harassment and discrimination.



5. Additional Rules of Engagement as a Corporate Social Media Publisher

- a. **In addition to following the Code of Conduct and Guiding Principles:**
- I. **Do not comment or engage others on non-Company Web sites or Social Media channels unless you are granted permission by The Company's corporate marketing group.** Corporate Marketing is responsible for all internal and external corporate communications. It is important corporate marketing knows what is being posted in the event they need to get involved due to any issues that may arise from a post or comment on a third party Web site. If you do have permission, review privacy settings of the social networking site you are using. Understand that when your content is posted on a public social network, all posts and comments may be traceable. Any information that you post should be considered at risk for public disclosure, regardless of your privacy settings since your postings can be reposted elsewhere and may be viewed by people other than your intended audience.
 - II. **Be authentic, factual and respectful at all times** Use your real identity. Provide informed, well-supported opinions and cite sources, if applicable. Always obtain permission if needed. Though Social Media sites are a more casual form of communication, be sure to remain professional and use a positive tone of voice. Be respectful of your colleagues, The Company, our customers, prospects and our competitors.
 - III. **Avoid engaging in on-line disputes with your audience.** Don't use slurs, personal insults or obscenity, and always respect privacy concerns. Avoid language that may be considered objectionable or inflammatory. Show that you have listened and be responsive. If you disagree, respond in professional and respectful manner.
 - IV. **Stick to your area of expertise** and provide unique, individual perspectives on what's going on at your business unit and in the world. In the event you cannot answer a question or comment, refer it to the appropriate internal contact.
 - V. **Post meaningful, respectful comments**—in other words, no spam and no remarks that are off-topic or offensive. Remember that some postings on the Internet can have an indefinite life and may not have the ability to be removed.
 - VI. **Please respect our Company Privacy Policy.** Do not disclose any information from anyone covered under our Company Privacy Policy.
 - VII. **Be aware of global implications. Your posts can have global significance.** The way that you answer an online question might be appropriate in some parts of the world, but inaccurate, inappropriate (or even illegal) in others. Keep that "world view" in mind when you are participating in online conversations. If you have a question about global relevance, please contact the appropriate PR Representative for guidance.
- b. **Setting up corporate spaces in Social Media channels**
- I. **To create a corporate account for a Social Media channel,** you must get permission from your director and submit the request to social.media@volarisgroup.com for approval. All accounts are managed from a corporate management center. This is to track accounts and not lose control of spaces once an employee leaves, or an administrator needs to access the account. Once approved, the corporate Web team will set up the appropriate account/space and access permission. We will also provide the necessary branding,



verbiage and disclaimer. A Company Social Media Playbook will be made available to you that will help you as a Company Social Media communicator.