College of New Caledonia
CNC

Privacy Impact Assessment

Sprout Social

PIA#21-008

Table of Contents

PART 1: GENERAL INFORMATION

PIA file number:

Initiative title:	Sprout Social
Organization:	College of New Caledonia
Branch or unit:	Communications Services
Your name and title:	Jo-Ann Bellamy, Privacy Consultant Hooper Access and Privacy Consulting Ltd.
Your work phone:	250-208-3431
Your email:	jbellamy@hooperconsulting.ca
Initiative Lead name and title:	Stephanie Deol Associate Director of Marketing, Brand, and Creative

Initiative Lead phone:	250-961-1691
Initiative Lead email:	Deols2@cnc.bc.ca
Privacy Officer:	
Privacy Officer phone:	
Privacy Officer email:	

General information about the PIA:

Is this initiative a data-linking program under FOIPPA? If this PIA addresses a data-linking program, you must submit this PIA to the Office of the Information and Privacy Commissioner.
No
Is this initiative a common or integrated program or activity? Under section FOIPPA 69 (5.4), you must submit this PIA to the Office of the Information and Privacy Commissioner.
No
Related PIAs, if any:
N/A

1. What is the initiative?

The CNC Communications Services Department is planning to replace its existing social media application, Hootsuite, with Sprout Social. Sprout Social is a web-based all-in-one social solution that provides higher education social marketers with publishing, engagement and analytics tools that help create meaningful connections with students. Sprout Social allows social media channel scheduling, batch content distribution, and analytics. The analytics provide quantitative and contextual data for all social profiles across Facebook, Twitter, Instagram, LinkedIn, and Google+. Sprout Social also has a suite of reports that can track metrics related to audience growth, reach, impressions, and engagement. Users can also create custom reports to easily track specific social data. Sprout Social also has a full suite of social media publishing tools that

make it easy to plan and schedule weeks of social content in advance, and automatically post content at times when the students are most engaged on social media.

2. What is the scope of the PIA?

This PIA addresses the collection, use, disclosure, storage, and security of personal information in the Sprout Social application.

3. What are the data or information elements involved in your initiative?

The data collected will include usernames and information that is sent through social media channels which could include personal information. Sprout Social will collect the information that is being posted on social media accounts (e.g., Facebook, Instagram, etc.). Information may include a user's social media handle, username, profile picture, biography, follower counts, website URL, first and last name (if provided by user), and messages or communications with the social media users.

3.1 Did you list personal information in question 3?

Personal information is any recorded information about an identifiable individual, other than business contact information. Personal information includes information that can be used to identify an individual through association or reference.

Yes.

- If yes, go to Part 2
- If no, answer question 4 and submit questions 1 to 4 to your Privacy Officer. You do not need to complete the rest of the PIA template.

4. How will you reduce the risk of unintentionally collecting personal information?

N/A

PART 2: COLLECTION, USE AND DISCLOSURE

This section will help you identify the legal authority for collecting, using, and disclosing personal information, and confirm that all personal information elements are necessary for the purpose of the initiative.

5. Collection, use and disclosure

Use column 2 to identify whether the action in column 1 is a collection, use or disclosure of personal information. Use columns 3 and 4 to identify the legal authority you have for the collection, use or disclosure.

Use this column to describe the way personal information moves through your initiative step by step as if you were explaining it to someone who does not know about your initiative.	**Collection, use or disclosure**	**FOIPPA authority**	**Other legal authority**
Step 1: Personal information is collected via Sprout Social from various social media channels.	Collection	26(c)	
Step 2: Personal information is used by CNC to engage with social media users, run reports, and perform analytics.	Use	32(a)	

6. Collection Notice

Following is the notification from CNC's Registration for Admission form which is currently being updated to include an additional purpose of "the ongoing administration of the student experience":

The information on this form and all required admissions and registration documentation is collected for the purpose of meeting the data requirements for admission, registration, research, alumni and development, statistical analysis, locker and U-Pass administration, and the student health plan. It is collected under the authority of the College and Institute Act and your privacy is protected under the Freedom of Information and Privacy Act limiting how your information may be used or disclosed. If you have any questions about the collection and use of your information contact the Freedom of Information Coordinator, College of New Caledonia at 250 561 5828.

PART 3: STORING PERSONAL INFORMATION

If you're storing personal information outside of Canada, identify the sensitivity of the personal information and where and how it will be stored.

7. Is any personal information stored outside of Canada?

Yes.

8. Does your initiative involve sensitive personal information?

Yes.

- If yes, go to question 9
- If no, go to question 10

9. Is the sensitive personal information being disclosed outside of Canada under FOIPPA section 33(2)(f)?

No.

- If yes, go to question 10
- If no, go to Part 4

10. Where are you storing the personal information involved in your initiative?

Customer data is hosted in AWS's us-east-1, North Virginia, USA.

After you answer this question go to Part 5.

PART 4: ASSESSMENT FOR DISCLOSURES OUTSIDE OF CANADA

Complete this section if you are disclosing sensitive personal information to be stored outside of Canada. You may need help from your organization's Privacy Officer.

11. Is the sensitive personal information stored by a service provider?

Yes.

- If yes, fill in the table below (add more rows if necessary) and go to question 13
- If no, go to question 12

Name of service provider	Name of cloud infrastructure and/or platform provider(s) (if applicable)	Where is the sensitive personal information stored (including backups)?
Sprout Social	Amazon Web Services	North Virginia, USA

12. Provide details on the disclosure, including to whom it is disclosed and where the sensitive personal information is stored.

Personal information is disclosed to Sprout Social in order to use their service. Personal information may include a user's social media handle, username, profile picture, biography, follower counts, website URL, first and last name (if provided by user), and messages or communications with Sprout Social's customers.

Customer data is hosted in AWS us-east-1 in North Virginia, USA.

13. Does the contract you rely on include privacy-related terms?

Yes.

- If yes, describe the contractual measures related to your initiative.

Sprout Social's Terms of Service, including Confidentiality and Data Privacy clauses, are located on their website at https://sproutsocial.com/terms/. Sprout Social also has a Data Processing Addendum which addresses international students maintaining an address in the European Union. Sprout Social's Privacy Policy details their collection, use, disclosure, storage, and security of personal information: https://sproutsocial.com/privacy-policy/

15. What controls are in place to prevent unauthorized access to sensitive personal information?

CNC

[redacted] 15(1)(l)

Sprout Social/AWS

Sprout Social is SOC 2 Type 2 compliant and as such have met all requirements regarding restricted access controls. [redacted] 15(1)(l)

AWS is SOC 2 Type 2 compliant and as such have met all requirements regarding restricted access controls. [redacted] 15(1)(l)

16. Provide details about how you will track access to sensitive personal information.

CNC

Access to Sprout Social will only be used by Communications staff and will be based on least privilege and need-to-know principles.

Sprout Social/AWS

Sprout Social/AWS provide continuous monitoring for unauthorized access through video surveillance, intrusion detection, and access log monitoring systems.

17. Describe the privacy risks for disclosure outside of Canada.

Use the table to indicate the privacy risks, potential impacts, likelihood of occurrence and level of privacy risk. For each privacy risk you identify describe a privacy risk response that is proportionate to the level of risk posed.

This may include reference to the measures to protect the sensitive personal information (contractual, technical, security, administrative and/or policy measures) you outlined. Add new rows if necessary.

Privacy risk	**Impact to individuals**	**Likelihood of unauthorized collection, use, disclosure or storage of the sensitive personal information (low, medium, high)**	**Level of privacy risk (low, medium, high, considering the impact and likelihood)**	**Risk response (this may include contractual mitigations, technical controls, and/or procedural and policy barriers)**	**Is there any outstanding risk? If yes, please describe.**
Unauthorized individuals at CNC access the personal information.	Low	Low	Low	Access will be restricted based on least privilege and need-to-know principles. Employees receive training regarding the confidentiality of student information.	No

Personal information is compromised during transmission.	Low	Low	Low	All communications over public networks with Sprout Social's application and API utilize [redacted] All data is store encrypted-at-rest with [redacted] including backups.	No 15(1)(l) 15(1)(l)
Unauthorized individuals at Sprout Social access the personal information.	Low	Low	Low	Sprout Social is SOC 2 Type 2 compliant. All new hires with access to customer data undergo a criminal history and background check prior to employment. All employees participate in annual general security and data privacy training. All employees must affirm their responsibilities in protecting customer data as part of their condition of employment.	No
Unauthorized individuals at AWS access the personal information.	Low	Low	Low	AWS is SOC 2 Type 2 compliant. Data centre buildings have strict physical access review and scrutiny. All physical access is monitored 24/7 by personnel.	No

				Multi-factor authentication is required for all visitors. Continuous monitoring for unauthorized access is done through video surveillance, intrusion detection, and access log monitoring systems.	

Outcome of Part 4

The outcome of Part 4 will be **a risk-based decision made by the head of the public body on whether to proceed with the initiative**, with consideration of the risks and risk responses, including consideration of the outstanding risks in question 17. **The public body may document the decision in an appropriate format as determined by the head of the public body or by using this PIA template.**

PART 5: SECURITY OF PERSONAL INFORMATION

In Part 5 you will share information about the privacy aspect of securing personal information. People, organizations, or governments outside of your initiative should not be able to access the personal information you collect, use, store or disclose. You need to make sure that the personal information is safely secured in both physical and technical environments.

18. Does your initiative involve digital tools, databases or information systems?

Yes.

- If yes, work with your Privacy Officer to determine whether you need a security assessment to ensure the initiative meets the reasonable security requirements of FOIPPA section 30

18.1 Do you or will you have a security assessment to help you ensure the initiative meets the security requirements of FOIPPA section 30?

Sprout Social and AWS are SOC 2 Type 2 compliant.

- If yes, you may want to append the security assessment to this PIA. Go to question 20
- If no, go to question 19

19. **What technical and physical security do you have in place to protect personal information?**

CNC

15(1)(l)

Sprout Social/AWS

Sprout Social's security policy can be found at https://sproutsocial.com/security/. Sprout Social has maintained SOC2, Type 2 certification since December 2019.

Sprout Social's products are hosted by Amazon Web Services (AWS). AWS is compliant with Cloud Security Alliance Star Level 2, ISO 9001, 27001, 27017, 27018, PCI DSS Level 1, and SOC 1, 2, and 3.

20. **Controlling and tracking access**

Strategy	
We only allow employees in certain roles access to information	Yes
Employees that need standing or recurring access to personal information must be approved by executive lead	Yes
We use audit logs to see who accesses a file and when	No

Strategy	
Describe any additional controls:	Sprout Social and AWS are SOC 2 Type 2 complaint and therefore have access controls in place.

PART 6: ACCURACY, CORRECTION AND RETENTION

In Part 6 you will demonstrate that you will make a reasonable effort to ensure the personal information that you have on file is accurate and complete.

21. How will you make sure that the personal information is accurate and complete?

Personal information is collected from individuals' social media accounts and posts. As such, individuals are responsible for the accuracy of their information.

22. Requests for correction

FOIPPA gives an individual the right to request correction of errors or omissions to their personal information. You must have a process in place to respond to these requests.

22.1 Do you have a process in place to correct personal information?

Yes. Individuals may make changes to their own social media accounts and feedback. Users who wish to access, correct, update or request deletion of their information collected by Sprout Social, can contact Sprout Social as per their Privacy Policy at https://sproutsocial.com/privacy-policy/

22.2 Sometimes it's not possible to correct the personal information. FOIPPA requires that you make a note on the record about the request for correction if you're not able to correct the record itself. Will you document the request to correct or annotate the record?

N/A – correction is possible as described above.

22.3 If you receive a request for correction from an individual and you know you disclosed their personal information in the last year, FOIPPA requires you to notify the other public body or third party of the request for correction. Will you ensure that you conduct these notifications when necessary?

N/A – personal information will not be disclosed to other public bodies or third parties.

23. Does your initiative use personal information to make decisions that directly affect an individual?

No.

- If yes, go to question 25
- If no, skip ahead to Part 7

24. Do you have an information schedule in place related to personal information used to make a decision?

N/A

PART 7: AGREEMENTS AND INFORMATION BANKS

Please provide information about whether your initiative will involve an information sharing agreement, research agreement or personal information bank.

25. Does your initiative involve an information sharing agreement?

No.

26. Will your initiative result in a personal information bank?

A personal information bank (PIB) is a collection of personal information searchable by name or unique identifier.

No.

- If yes, please complete the table below.

Describe the type of information in the bank
Name of main organization involved
Any other ministries, agencies, public bodies or organizations involved
Business contact title and phone number for person responsible for managing the PIB

PART 8: ADDITIONAL RISKS

Part 8 asks that you reflect on the risks to personal information in your initiative and list any risks that have not already been addressed by the questions in the template.

27. Risk response

Describe any additional risks that arise from collecting, using, storing, accessing or disclosing personal information in your initiative that have not been addressed by the questions on the template.

N/A. See #17 for identified risks and mitigations.

Possible risk	Response

PART 9: SIGNATURES

You have completed a PIA. Submit the PIA to your Privacy Officer for review and comment, and then have the PIA signed by those responsible for the initiative.

Privacy Office Comments

Privacy Office Signatures

This PIA is based on a review of the material provided to the Privacy Office as of the date below.

Role	Name	Signature	Date signed
Privacy Consultant	Bev Hooper, Hooper Access and Privacy Consulting Ltd.	[redacted]	Jan 28/22 22(1)

Program Area Signatures

This PIA accurately documents the data elements and information flow at the time of signing. If there are any changes to the overall initiative, including to the way personal information is collected, used, stored or disclosed, the program area will engage with their Privacy Office and if necessary, complete a PIA update.

Program Area Comments:

Role	Name	Signature	Date signed	
Initiative lead	Stephanie Deol Associate Director of Marketing, Brand, and Creative	[redacted]	Jan. 31/22	22(1)
Program/Department Manager				
Contact Responsible for Systems Maintenance and/or Security Only required if they have been involved in the PIA				
Head of public body, or designate Only required if personal information is involved	David Loewen Director, PPS.	[redacted]	Mar. 3/22	22(1)