

## **BAND Standard Student Data Privacy Agreement**

This BAND Standard Student Data Privacy Agreement (“DPA”) is hereby entered into on this \_\_\_\_ day of \_\_\_\_\_, \_\_\_\_\_, between Naver U.Hub dba NAVER BAND (“Provider”), a provider of the BAND application, and \_\_\_\_\_ (“LEA”), a local educational agency.

**1. DEFINITIONS.** For purposes of this DPA, the following terms have the meanings set forth below:

- 1.1. “**Administrative Contact**” means the administrative contact for LEA identified below, or as updated by LEA by written notice to Provider.
- 1.2. “**Data Breach**” means an unauthorized release, access to, disclosure, or acquisition of Student Data that compromises the security, confidentiality, or integrity of the Student Data maintained by Provider in violation of applicable of state or federal law.
- 1.3. “**De-Identified Data**”: Records or information are considered to be De-Identified when all PII has been removed or obscured, such that the remaining information does not reasonably identify a specific student, including, but not limited to, any information that, alone or in combination, is linkable to a specific student.
- 1.4. “**Education Record**” has the meaning set forth under FERPA at 20 U.S.C. § 1232g(a)(5)(A).
- 1.5. “**FERPA**” means the Family Educational Rights and Privacy Act, 20 U.S.C. § 1232g, and its implementing regulations enacted at 34 C.F.R. Part 99.
- 1.6. “**Personally Identifiable Information**” (“**PII**”) has the same meaning as defined under FERPA at 34 C.F.R. § 99.3. To the extent that LEA provides Provider with Personal Information from U.S. residents in connection with the Services, PII will have the same meanings as in applicable Privacy Laws, and their related terms will be construed accordingly.
- 1.7. “**Privacy Laws**” means all applicable laws and binding rules or regulations relating to the processing of PII applicable to either party in connection with its use or provision of the Services, each as amended or replaced from time to time, including without limitation the California Consumer Privacy Act, Cal. Civ. Code §§ 1798.100 et seq., as amended by the California Privacy Rights Act of 2020 (“**CCPA**”), state consumer privacy laws, and state student privacy laws.

- 1.8. **“School Official”** has the same meaning as under FERPA at 34 C.F.R. § 99.31(a)(1), and includes contractors, consultants, volunteers, or other parties to which an LEA has outsourced institutional services or functions.
- 1.9. **“Service Agreement”** means any underlying quote, contract, purchase order, terms of service, and/or terms of use agreed between the parties that governs the provision of the Services from Provider to LEA.
- 1.10. **“Services”** means the BAND application or BAND for Kids application to the extent that it is used by LEA in connection with LEA’s communications with Students within the Bands designated as “School Bands” by LEA.
- 1.11. **“Student”** means a student enrolled at LEA using a Student Account.
- 1.12. **“Student Account”** means an account for an individual registered as a “Student,” which permits access to the Services for educational purposes.
- 1.13. **“Student Data”** means any data, whether gathered, created or inferred by Provider or provided by LEA or its users, students, or students’ parents/guardians, for a school purpose, that is descriptive of the student including, but not limited to, information in the student’s Education Record, persistent unique identifiers, or any other information or identification number that would provide information about a specific student. Student Data further includes PII if it relates to an identified or identifiable Student. Student Data does not include De-Identified Data or anonymous usage data regarding a student’s or LEA’s use of the Services. Student Data is limited to data within the Bands designated as “School Bands” and excludes data not provided or used in the context of providing the Services to LEA.
- 1.14. **“Student-Generated Content”** means materials or content created by a student using the Services including, but not limited to, essays, research reports, portfolios, creative writing, music or other audio files, photographs, and videos. “Student Generated Content” does not include student responses to a standardized assessment where student possession and control would jeopardize the validity and reliability of that assessment. “Student Generated Content” is limited to materials or content created in connection with School Bands.
- 1.15. **“Subprocessor”** means a party other than LEA or Provider, which Provider or its affiliates use for data collection, analytics, storage, or other service to operate, analyze, or improve the Services, and which has access to or storage of Student Data.

## 2. GENERAL

- 2.1. Provider agrees that all Student Data, along with its intellectual property rights, including any copies or modifications transferred to Provider under any Service Agreement, remain the property and under the control of LEA and/or Students, as determined by applicable law, and not Provider.
- 2.2. Parents, legal guardians, or Students who have reached the age of majority can request access to and corrections of Education Records and/or Student Data stored by the Services by making these requests to LEA, which will provide them to Provider as necessary. Provider will promptly respond to LEA's requests for Student Data and will address such requests in a timely manner and as required by applicable Privacy Laws. If an individual contacts Provider directly to access or correct Student Data, Provider will put them in contact with LEA for processing of their request.
- 2.3. Administrative Contact can make requests to access or correct Student Data to Provider on behalf of LEA, a legal guardian, or a Student by providing Provider with the Student's name and email address for the applicable Student Account. Where it does so, LEA will verify the identity of the Student, including Student's enrollment at LEA, and the legal guardian as applicable. This provision is limited to School Officials with legitimate educational interests as permitted by FERPA.
- 2.4. If law enforcement or other government entities contact Provider to request Student Data held as part of the Services, Provider will notify LEA beforehand before disclosing any data, unless explicitly instructed otherwise by the lawful authority or otherwise prohibited by law.
- 2.5. Upon request from LEA, Provider will facilitate the transfer of Student Data and Student-Generated Content to a separate account designated by LEA, or provide a mechanism for LEA to do so.
- 2.6. Provider will maintain a list of all Subprocessors on a publicly available webpage.

### **3. RESPONSIBILITIES OF PROVIDER**

- 3.1. Provider agrees to provide the Services consistent with the requirements of applicable Privacy Laws.
- 3.2. Provider agrees that to the extent that LEA is subject to FERPA and provides Provider with Student Data in connection with the Services, Provider will be considered a School Official.
- 3.3. The Student Data processed by Provider under this DPA, including persistent unique identifiers, will be used for no purpose other than to provide the Services and for other purposes listed in this DPA, or as instructed by LEA.

- 3.4. Provider agrees that to the extent that LEA provides Provider with Student Data from U.S. residents in connection with the Services, Provider will process such U.S. Student Data as a “service provider” or “processor” to LEA with respect to such Student Data, as those terms are defined by applicable Privacy Laws. The processing will be carried out for the purpose of provisioning the Services and for the duration set forth in this DPA, and Provider will:
- (a) assist LEA, taking into account the nature of the processing, (i) by appropriate technical and organizational measures and where possible, in fulfilling LEA’s obligations to respond to requests from data subjects exercising their rights under applicable Privacy Laws; and (ii) by making available to LEA all information reasonably requested by LEA for the purpose of demonstrating compliance with applicable Privacy Laws;
  - (b) allow LEA and LEA’s authorized representatives to access and review up-to-date attestations, reports, or extracts thereof from independent bodies (e.g., external auditors, data protection auditors) or suitable certifications, or to conduct audits or inspections to ensure compliance with the terms of this DPA. Any audit or inspection will be conducted during Provider’s regular business hours, with reasonable advance notice to Provider and subject to reasonable confidentiality procedures. In addition, audits or inspections will be limited to once per year; and
  - (c) notify LEA if, in Provider’s opinion, an instruction for the processing of Student Data infringes applicable Privacy Laws.

Provider will not combine Student Data collected as a service provider or processor with data received from other businesses or collected in Provider’s own business capacity.

- 3.5. Provider acknowledges that LEA and/or Students are the owner of Student Data provided by LEA through the Services, as determined by applicable law, and not Provider.
- 3.6. Provider will collect, use, and otherwise process Student Data provided by LEA through the Services only as described in this DPA and the BAND Privacy Statement available at <https://band.us/policy/school-use-privacy> and (if Students use BAND for Kids application as they are under the age of 13) and <https://band.us/policy/coppa-privacy>, which are incorporated into this DPA by reference. This includes features which may allow Students to post PII and Student-Generated Content to interactive features on the Services, which may be viewed by other users within LEA. Provider will not (i) use Student Data for any purposes not specified in this DPA, or not authorized by the parent/guardian or LEA, (ii) use, disclose, or sell Student Data for targeted advertising or targeted

marketing purposes; (iii) use Student Data to amass a profile about a student except in furtherance of the Services; (iv) sell Student Data, or (v) disclose Student Data, unless permitted by this DPA, by law, or upon approval of LEA. Provider will not collect more information than is reasonably necessary in order to provide the Services.

- 3.7. Provider acknowledges and agrees to not disclose any Student Data or its components, including Student-Generated Content or PII, except as instructed or permitted by LEA or this DPA. This restriction does not apply to aggregate summaries of De-Identified Data, Student Data disclosed under a lawfully issued subpoena or legal process, or to Subprocessors working on behalf of Provider under this DPA.
- 3.8. Provider commits to not attempt to re-identify De-Identified Data. Such data may be utilized by Provider for purposes permitted under FERPA and for specific reasons, including assisting LEA or governmental agencies in research, developing educational sites or services, demonstrating the effectiveness of the Services, adaptive learning, and customized student learning. Provider's use of De-Identified Data may continue even after termination of the Service Agreement, this DPA, or any request by LEA to return or destroy Student Data. Except for Subprocessors, Provider agrees to not transfer De-Identified Data to any party unless the party agrees in writing to not attempt re-identification and prior written consent has been obtained from LEA. Before publishing any document mentioning LEA directly or indirectly, Provider must obtain written approval from LEA regarding the publication of De-Identified Data.
- 3.9. Provider will require all employees and agents who have access to Student Data to comply with all applicable provisions of this DPA and to maintain the confidentiality of Student Data.
- 3.10. To the extent that Provider engages Subprocessors to process Student Data as part of the delivery of the Services, Provider will enter into written agreements with all such Subprocessors requiring that the Subprocessors process the Student Data in accordance with this DPA, and apply security measures to Student Data no less stringent than those specified in this DPA.
- 3.11. To the extent that Provider collects Student Data directly from Student, Provider will obtain the consent of the Student, or Students' parents/guardians if the Student is less than the age of majority, before using Student Data in a manner that conflicts with this DPA, and when it collects Student Data from an individual or entity other than the Student, will obtain the consent of LEA before using Student Data in a manner that conflicts with this DPA.

- 3.12. Provider agrees that it will destroy Student Data or Student-Generated Content provided through the Services within its possession, custody, or control within ninety (90) days following the time that the corresponding Student Account is deleted. Notwithstanding the foregoing, Provider will be permitted to retain an archival copy of the Student Data or Student-Generated Content as may be required or permitted by law, including where instructed by a legal guardian or Student who has reached the age of majority.
- 3.13. Provider will provide LEA with a means to delete or facilitate the transfer of Student Data under this DPA to enable LEA to delete Student Data at any point. If this DPA is terminated and no written request is received from LEA, Provider will delete all Student Data after providing reasonable prior notice to LEA. However, this obligation does not extend to De-Identified Data or data stored outside of a School Band.

#### **4. RESPONSIBILITIES OF LEA**

- 4.1. LEA will use the Services consistent with the requirements of applicable Privacy Laws
- 4.2. Prior to Students' use of the Services, LEA will gather any parent/guardian consent, or provide such consent on behalf of parents/guardians if permitted, to the extent such consent is required by applicable law.
- 4.3. LEA will ensure that any Student Data it discloses to Provider, or authorizes Provider to collect and use, for the purposes specified by this DPA is in compliance with all applicable Privacy Laws.
- 4.4. Upon executing this DPA, Provider will supply LEA with a customized registration link. This link allows LEA and its employees to register their Band groups as part of the School Band. It is the exclusive responsibility of LEA, its employees, and affiliated staff to complete the registration process on the Services to ensure their groups are included in the School Band. Consequently, the content and data associated with the School Band that is Student Data will become subject to this DPA.
- 4.5. LEA, its employees, and affiliated staff will take reasonable precautions to secure usernames, passwords, and any other means of gaining access to the Services and hosted Student Data.
- 4.6. LEA will notify Provider promptly of any known unauthorized access to Student Data. LEA will assist Provider in any efforts by Provider to investigate and respond to any unauthorized access.
- 4.7. LEA hereby consents to Provider's collection, use, and disclosure of Student Data, as described in Provider's direct notices of privacy practices on

Provider's website at <https://band.us/policy/coppa-privacy>, if Students use BAND for Kids application as they are under the age of 13, and <https://band.us/policy/school-use-privacy>, as agent on behalf of the parents/ guardians of Students who use the Services. In doing so, LEA represents that it has obtained sufficient authorization from those parents/ guardians to provide consent on their behalf, and that it will make Provider's direct notice of information practices available to those parents/guardians as appropriate.

## **5. DATA SECURITY**

- 5.1. Provider agrees to protect and maintain Student Data with commercially reasonable security measures that include appropriate administrative, physical, and technical safeguards to secure Student Data from unauthorized access, disclosure, and use.
- 5.2. Provider agrees to use best practices to secure usernames, passwords, and any other means of gaining access to the Services or Student Data.
- 5.3. When the Services are accessed using a supported web browser, Provider agrees to use Hyper Text Transfer Secure (HTTPS) technology, which uses both server authentication and data encryption to help keep Student Data secure.
- 5.4. Provider agrees to maintain security protocols that meet industry best practices in the transfer or transmission of data related to the Services, including that data may only be viewed or accessed by parties authorized to do so.
- 5.5. Provider agrees to provide periodic security training to employees who process Student Data, and require such employees to comply with applicable student privacy laws.
- 5.6. Provider agrees to conduct periodic risk assessments of the Services. In the event of unauthorized access, Provider will permit LEA to conduct an audit of security and privacy measures and cooperate with LEA and relevant authorities, providing access to facilities, staff, data, and records pertaining to the delivery of the Services as needed to investigate the unauthorized access.
- 5.7. When hosting Student Data, Provider agrees to host such data in an environment using a firewall that is periodically updated according to industry standards.
- 5.8. In the event of a verified Data Breach arising from Provider's provision of the Services, Provider will notify the affected Student and LEA in compliance with applicable law as related to the Data Breach. Actions following a Data Breach may also include a summary of remediation actions, depending on incident type.
- 5.9. If Provider becomes compelled by law or regulation, subpoena, court order, or other administrative directive to disclose any Student Data, Provider will

provide Student and LEA with prompt written notice, to the extent permitted by law and to the extent that the Student maintains accurate school information in their Student Account, so that Student or LEA may seek an appropriate protective order or other remedy. If a remedy acceptable to Student or LEA is not obtained by the date that Provider will comply with the request, Provider will furnish only that portion of the Student Data that it is legally required to furnish, and Provider will take reasonable steps to require the recipient of the Student Data to exercise commercially reasonable efforts to keep the Student Data confidential, to the extent permitted by law.

## 6. MISCELLANEOUS

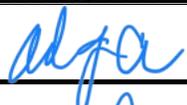
- 6.1. **Term.** The term of this DPA will commence on the date specified below and terminate in accordance with the terms of this DPA.
- 6.2. **Termination.** Either party may terminate this DPA upon 90 days prior written notice to the other party. Prior to the expiration of such 90-day period, LEA will delete, or will instruct Students to delete, any Student Data or Student-Generated Content provided by LEA or Students pursuant to this DPA that is required to be deleted under applicable law or LEA's policies and ensure such deletions are made. If LEA or Students cannot delete such Student Data or Student-Generated Content, they will reach out to Provider for assistance.
- 6.3. **Changes to Terms.** To the maximum extent permitted by applicable law, Provider reserves the right from time to time to (and LEA acknowledges that Provider may) modify this DPA as set forth in this Section. Provider will notify LEA in writing (the "Modification Notice") of the modification to this DPA (the "Modified Agreement"). If LEA does not agree to the terms of the Modified Agreement, it may reject the modification by notifying Provider in writing of the rejection within 30 days of the Modification Notice. If LEA rejects a modification under these circumstances, its access to and use of the Services will continue to be governed by this DPA in effect immediately before the modification until 90 days after the Modification Notice. Within such 90-day period, LEA will delete, or will instruct Students to delete, all Student Data and ensure such deletions are made. Use of the Services after such 90-day period will be under the terms of the Modified Agreement. Notwithstanding the foregoing, modifications to the Privacy Statement will be handled as described therein.
- 6.4. **Notice.** All notices or other communication required or permitted to be given hereunder will be in writing and given by e-mail transmission sent to/from [dl\\_schoolband@navercorp.com](mailto:dl_schoolband@navercorp.com). Notifications to LEA will be provided via email to the Administrative Contact.
- 6.5. **Entire Agreement.** This DPA and the Service Agreement(s) constitute the entire agreement of the parties relating to the subject matter hereof and supersede all prior communications, representations, or agreements, oral or written, by the parties relating thereto. In the event there is conflict between the

terms of this DPA and the Service Agreement(s), the terms of this DPA will apply and take precedence. Neither failure nor delay on the part of any party in exercising any right, power, or privilege hereunder will operate as a waiver of such right, nor will any single or partial exercise of any such right, power, or privilege preclude any further exercise thereof or the exercise of any other right, power, or privilege. Neither party will assign this DPA or any right, interest, or benefit under this DPA, without the prior written consent of the other party, provided that Provider may, without prior consent, assign or transfer this DPA to an affiliate or in connection with a merger, change of control, reorganization or sale or other disposition of the Services or assets related to the Services.

- 6.6. **Severability.** Any provision of this DPA that is prohibited or unenforceable in any jurisdiction will, as to such jurisdiction, be ineffective to the extent of such prohibition or unenforceability without invalidating the remaining provisions of this DPA, and any such prohibition or unenforceability in any jurisdiction will not invalidate or render unenforceable such provision in any other jurisdiction. Notwithstanding the foregoing, if such provision could be more narrowly drawn so as to not be prohibited or unenforceable in such jurisdiction while, at the same time, maintaining the intent of the parties, it will, as to such jurisdiction, be so narrowly drawn without invalidating the remaining provisions of this DPA or affecting the validity or enforceability of such provision in any other jurisdiction.

**This DPA must be signed by an authorized representative of LEA and delivered to Provider at [dl\\_schoolband@navercorp.com](mailto:dl_schoolband@navercorp.com).**

Name of LEA: BLUFORD UNIT SCHOOL DISTRICT 318

Authorized Signature: 

Name and Title of Signatory: ADAM J. CROSS, SUPERINTENDENT

Administrative Contact Name: ADAM J. CROSS

Administrative Contact Phone: 618-732-8242

Administrative Contact Email Address: ACROSS@blufordschools.org

LEA Address: SAME AS ABOVE

**NAVER U.Hub Inc.**

**By:** *Goonji Chae*

**Name:** \_\_\_\_\_

**Title:** \_\_\_\_\_