Privacy and Security

Statement for All BRT applications, including the easyCBM editions (Lite, Teacher Deluxe, & District), WriteRightNow!, LRA-Greenhouse, and CORE.

Privacy and security are among the highest priorities for BRT and our applications, including the easyCBM editions (Lite, Teacher Deluxe, & District), WriteRightNow!, LRA-Greenhouse, and CORE. We work diligently to maintain student and faculty privacy and treat all sensitive data and personal information with the highest industry standards. This Privacy & Security Statement outline the specific steps that are taken to assure that student and faculty/staff data are treated carefully and appropriately.

Privacy

The protection of student, staff, and family personal information is critical to our work. As such, BRT has endorsed the Student Privacy Pledge, a strong set of commitments drafted with the involvement of educational non-profit groups, the Software & Information Industry Association, and public sector educational leaders. The easyCBM system, WriteRightNow!, LRA-Greenhouse, and CORE are run by Behavioral Research and Teaching, a research center in the University of Oregon's College of Education. As part of a public research university we are ineligible to be a signatory to the pledge but have committed to following each aspect of the pledge completely. This privacy statement outlines our commitments and the steps we take to ensure that personal (i.e., individually identifiable) information remains private.

As per the Student Privacy Pledge, BRT commits to:

- Not collect, maintain, use or share student personal information beyond that needed for authorized educational/school purposes, or as authorized by the parent/student.
- Not sell student personal information.
- Not use or disclose student information collected through an educational/school service (whether personal information or otherwise) for behavioral targeting of advertisements to students.
- Not build a personal profile of a student other than for supporting authorized educational/school purposes or as authorized by the parent/student.
- Not make material changes to school service provider consumer privacy policies without first providing prominent notice to the account holder(s) (i.e., the educational institution/agency, or the parent/student when the information is collected directly from the student with student/parent consent) and allowing them choices before data are used in any manner inconsistent with terms they were initially provided; and not make material changes to other policies or practices governing the use of student personal information that are inconsistent with contractual requirements.
- Not knowingly retain student personal information beyond the time period required to support the authorized educational/school purposes, or as authorized by the parent/student.

Note: Any information held in secure backup files beyond license expiration will be deleted over time through normal backup procedures in keeping with Federal regulations related to federally-funded projects.

- Collect, use, share, and retain student personal information only for purposes for which we were authorized by the educational institution/agency, teacher or the parent/student.

- Disclose clearly in contracts or privacy policies, including in a manner easy for parents to understand, what types of student personal information we collect, if any, and the purposes for which the information we maintain is used or shared with third parties.

  Note: The easyCBM License Agreement details what personal information we collect and how it is used.

- Support access to and correction of student personally identifiable information by the student or their authorized parent, either by assisting the educational institution in meeting its requirements or directly when the information is collected directly from the student with student/parent consent.

  Note: Parents, guardians, or students may review and request changes to such data by communicating with their school.

- Maintain a comprehensive security program that is reasonably designed to protect the security, privacy, confidentiality, and integrity of student personal information against risks – such as unauthorized access or use, or unintended or inappropriate disclosure – through the use of administrative, technological, and physical safeguards appropriate to the sensitivity of the information. For more information, see our security statement below.

- Require that our vendors with whom student personal information is shared in order to deliver the educational service, if any, are obligated to implement these same commitments for the given student personal information.

  Note: We do not share student personal information with vendors except by specific request and authorization of the licensee.

- Allow a successor entity to maintain the student personal information, in the case of our merger or acquisition by another entity, provided the successor entity is subject to these same commitments for the previously collected student personal information.

Security

- **Secure Login and Password**. Security of data are enhanced through the use of a personal login and password. Logins are available only to a limited number of individuals selected by the site (i.e., specifically designated by a School, District, or State agency). Passwords are stored encrypted.

- **Encrypted Connection**. Information sent to or from our applications is encrypted in route to minimize the remote chance that the data could be re-routed and interpreted. Data are encrypted using SSL/TLS end-to-end encryption.

- **Firewall Protection.** BRT servers are housed behind firewalls which are secure, updated regularly, and continuously monitored.

- **Protection of Confidential Data.** The data entered by a school are only accessible by the school's designated account holders, BRT systems administrators, and BRT researchers who have successfully completed training on the protection of human subjects and educational research data.

Data Property

All information, data, and other content transmitted by the Licensee to BRT, or entered or uploaded under Licensee's user accounts, remain the sole property of the Licensee. The Licensee retains exclusive control over student and staff data, including determining who may access data and how it may be used for legitimate authorized purposes. BRT and the Licensee shall establish reasonable procedures by which a parent, legal guardian or eligible student may review personally identifiable information on the pupil's records, correct erroneous information, and procedures for the transfer of pupil-generated content to a personal account.

We welcome questions and comments related to the privacy and security of information entered into any of our applications. If you have additional questions or suggestions, please contact email support@easycbm.com or call us at 541-346-3535.