

Addendum B

PARENTS' BILL OF RIGHTS – SUPPLEMENTAL INFORMATION ADDENDUM

1. **EXCLUSIVE PURPOSES FOR DATA USE:** The exclusive purposes for which “student data” or “teacher or principal data” (as those terms are defined in Education Law Section 2-d and collectively referred to as the “Confidential Data”) will be used by **GimKit** (the “Vendor”) are limited to the purposes authorized in the contract between the vendor and the East Irondequoit Central School District (the “School District”) dated **May 7, 2020** (the “Contract”).
2. **SUBCONTRACTOR OVERSIGHT DETAILS:** The Vendor will ensure that any subcontractors, or other authorized persons or entities to whom the Vendor will disclose the Confidential Data, if any, are contractually required to abide by all applicable data protection and security requirements, including but not limited to those outlined in applicable state and federal laws and regulations (e.g., Family Educational Rights and Privacy Act (“FERPA”); Education Law §2-d; 8 NYCRR Part 121).
3. **CONTRACT PRACTICES:** The Contract commences and expires on the dates set forth in the Contract, unless earlier terminated or renewed pursuant to the terms of the Contract. On or before the date the Contract expires, protected data will be exported to the School District in **Desired secure method** format and/or destroyed by the Vendor as directed by the School District.
4. **DATA ACCURACY/CORRECTION PRACTICES:** A parent or eligible student can challenge the accuracy of any “education record”, as that term is defined in the FERPA, stored by the School District in a Vendor’s product and/or service by following the School District’s procedure for requesting the amendment of education records under the FERPA. Teachers and principals may be able to challenge the accuracy of APPR data stored by School District in Vendor’s product and/or service by following the appeal procedure in the School District’s APPR Plan. Unless otherwise required above or by other applicable law, challenges to the accuracy of the Confidential Data shall not be permitted.
5. **SECURITY PRACTICES:** Confidential Data provided to Vendor by the School District will be stored at **AWS (Amazon Web Services) and is encrypted at rest using those services**. The measures that Vendor takes to protect Confidential Data will align with the NIST Cybersecurity Framework including, but not necessarily limited to, disk encryption, file encryption, firewalls, and password protection. **Gimkit is built on Heroku, and Gimkit data is secured with best practices and is encrypted.**
6. **ENCRYPTION PRACTICES:** The Vendor will apply encryption to the Confidential Data while in motion and at rest at least to the extent required by Education Law Section 2-d and other applicable law.