BIDS: Please mail a sealed bid to the address below. We will open bids starting at 8:00am CST on August 16, 2019. Bid selection criteria will include cost, customer support, references/reputation, and ability to deliver RFP requirements below.

Hopkins County Schools
C\O Drew Taylor
320 South Seminary Street
Madisonville, KY 42431

At a minimum, the vendor:

1. Must provide pricing that includes the cost of the software/hardware, unlimited sex offender checks, maintenance, customer support, project management, training and implementation, including all costs related to the implementation of a complete turn-key administrative system solution, updates, installation and implementation in the pricing.
2. Must include pricing for 16 Schools and 1 Central Office.
3. Must verify that the proposed solution is implemented district wide in at least 100 other districts with 15 schools or more.
4. Must provide training and installation assistance for each school.
5. Must provide live customer support during regular school hours at no extra cost.
6. Must provide example written guidance from other school districts on policies and procedures to implement the system.

At a minimum, the Visitor Management System:

1. Shall be a web-based application.
2. Shall be capable of running on a standard configured desktop personal computer with broadband access to the Internet.
3. Shall be capable of being used by multiple internet browsers, to include Internet Explorer and Chrome.
4. Must be able to sign in and sign out visitors to a campus or District facility. This shall be done at a minimum by scanning a valid identification in one scan of the item such as a driver's license, identification card, military identification, or other legally recognized form of identification.
5. Must not allow for self-sign in on the first visit.
6. Must save prior visitor information for quick retrieval.
7. Must provide up-to-date information about who is currently on site, the area of the facility where they should be located, and the time that they entered.
8. Must be able to set custom alerts on individuals (such as banned visitors, restricted access, restraining order, custody issues, etc.).
9. Must have the ability to instantly and automatically check the visitor's information against the registered sex offender databases of all 50 United States at no additional cost. If a visitor is found in one of the databases to have a history as a registered sex offender, the System shall

automatically notify the attendant on their computer monitor of the alert, and electronically notify by email or text message a specific individual or individuals of the alert.
10. Must update the information in the offender databases at a minimum of once per week.
11. Must have False Positive Logic to eliminate false positive sex offender matches so that non-sex offender visitors do not get flagged on future visits to that school.
12. Must generate a printed badge on an adhesive backed paper media that will include, at a minimum, the visitor's name, picture or digital photo, destination or person they will be visiting, barcode, and date and time when the badge was issued.
13. Must have an Emergency Button, which operates as a silent alarm.
14. Shall provide the ability to print badges ahead of time for groups of visitors.
15. Shall have visual guardian matching for student early dismissals.
16. Must provide standard reports.
17. Must allow for custom reports to be created.

At a minimum, the Volunteer Management System:

1. Shall provide full volunteer management, including online volunteer applications, event management, built in email communications, volunteer tracking, and volunteer reporting.
2. Must be able to offer integrated FCRA compliant background checks for volunteers in the application process.
3. Shall provide an online community for volunteers to track their hours, sign up for events, communicate with each other and communicate with the district.
4. Must provide full reports on information captured by the system.
5. Must allow for custom reports to be created.

At a minimum, the Emergency Management System:

1. Must encrypt all data transmissions both at rest and in transit.
2. Must provide for varying level of user privileges based on credentials to at least include a distinct level for Incident Commander.
3. Must be compatible with IOS and Android smartphones and tablets.
4. Must allow for import of data through a Microsoft compatible desktop computer utilizing multiple internet browsers, to include Internet Explorer and Chrome.
5. Must allow for the import of class rosters.
6. Must allow for the import of student emergency contact data.
7. Must allow for the import of student approved guardians.
8. Must allow for the import of faculty emergency contact data.
9. Must send both emails and texts to a customized list of recipients upon the initial of both a drill and/or a live emergency.
10. Must allow for access to district emergency management documents in PDF form via a mobile device.
11. Must allow for students to be listed based on a class roster for a specific faculty member at a given schedule/period.
12. Must allow for users to account for the status of students in real time, to include accounted for, absent, missing, injured statuses as well as custom statuses.
13. Must allow for users to account for the status of faculty in real time, to include accounted for, absent, missing, injured statuses as well as custom statuses.

14. Must allow for users to account for the location of students in real time.
15. Must allow for users to account for the location of faculty in real time.
16. Must allow for users to search for individual students by name.
17. Must allow for users to search for individual faculty members by name.
18. Must allow for users to view all others in the buildings at the time of the incident (to include visitors, vendors, contractors, and volunteers).
19. Must provide Incident Commander dashboards to include summaries of student status and locations.
20. Must provide Incident Commander dashboards to include a summary of all active and inactive users during the drill/emergency.
21. Must be compatible with the Standard Response Protocol.
22. Must allow for the initiation of drills within the application.
23. Must allow for the initiation of live emergencies within the application.
24. Must be compatible with the Standard Reunification Method.
25. Must provide for the role of a Greeter within a reunification.
26. Must provide for the role of a Runner within a reunification.
27. Must provide for the role of a Reunifier within a reunification.
28. Must record whether a Guardian ID was verified by a Greeter, to include the name of the greeter and the date/time of the verification.
29. Must record whether a Guardian ID was verified by a Runner/Reunifier, to include the name of the Runner/Reunifier and the date/time of the verification.
30. Must allow for the capture of the Guardian signature during reunification.
31. Must have the ability to alert via text and/or email all other approved guardians for a student once the student is reunified.
32. Must delete all protected student and faculty data from the device upon the closing of an emergency.
33. Must provide standard reports for all drills performed by building and/or district.
34. Must provide standard reports for all live emergencies by building and/or district.
35. Must provide standard reports for all buildings which have not performed drills during a given time period.
36. Must allow for custom reports to be created.