G360

DATA BREACH AND PROTECTION

School corporations store a number of educational records in electronic data systems and have a legal and ethical responsibility to protect the privacy and security of that data, including personally identifiable information (PII), under the Family Education Rights and Privacy Act FERPA). It is the expectation of the Board of School Trustees that School Corporation employees and students understand their role in preventing data breaches and that employees understand their responsibility should a data breach occur.

Indiana law (IC 24-4.9) requires that Indiana residents be notified if a security breach has resulted in exposure of their personal information, defined as a social security number or name in combination with a driver's license number, account number, state identification card number, credit card number, financial account number or debit card number in combination with any required security code. Should such a security breach occur, the School Corporation will notify affected persons by mail, telephone or email.

Should an employee or student become aware of a data breach, they are asked to notify the [director of technology] as soon as possible. The Director of Technology will coordinate with the superintendent, Business Manager and building level administrator (if applicable) to ensure that the breach is quickly addressed and that any required notification is sent. The Business Manager will ensure that an appropriate separation of duties is in place to secure financial data. The Director of Technology will ensure that only specified users have access to PII and that accounts are managed appropriately and deactivated when necessary.

The School Corporation will provide regular training on privacy and information security to all employees to ensure they are aware of protocols for recognizing and reporting data breaches and attempted data breaches.

Greenfield-Central Community School Corporation

Adopted: 8/12/2024
Revised: [date]