Woodstock School District 200
2990 Raffel Road
Woodstock, IL 60098
Tel: 815.338.8204
Fax: 815.338.2005
George Oslovich
Director of Information Services
goslovich@wcusd200.org

May 8, 2026

Re: Canvas Data Breach

Dear District 200 Families:

We were informed this week by Instructure Inc, the parent company of Canvas, of a recent data breach within their Canvas Learning Management System. The data breach allowed unauthorized access to certain information stored within their systems. According to the investigation, the data potentially accessed included:

- student names
- email addresses,
- student ID numbers
- Canvas messages between users.

Their investigation so far does not indicate that passwords, dates of birth, government identifiers, or financial information were involved.

District 200 takes data security very seriously and our Technology Department has measures in place to safeguard our systems. Some of which include:

- Enforce Two-Factor Authentication and require all staff members to verify their identity with a second factor, such as a security key or text message authentication, to access their network account and other critical applications.
- Restrict students' ability to send or receive email from anyone outside District 200.
- Use access level security best practices and internal controls that restrict who has rights to view, add/delete, or edit information.
- Employ automated access management to remove access for employees who leave the district or change positions.
- Follow cybersecurity best practices, including regular updates, strong password policies, and system monitoring to prevent unauthorized access.
- Restrict and disable remote technical support access to mitigate risks from third-party systems to protect against incidents like this.
- Consult with federal, state, and private cybersecurity experts to review and enhance our cybersecurity posture.

We want to assure you that protecting our student data remains paramount. If you have any questions about this incident or general concerns regarding Canvas or student data, please contact our Technology Department at datasupport@wcusd200.org.

George Oslovich
Director of Information Services
March 13, 2023

Estimadas familias del Distrito 200:

Esta semana fuimos informados por Instructure Inc., la empresa matriz de Canvas, sobre una reciente violación de datos ocurrida dentro de su Sistema de Gestión del Aprendizaje (LMS) Canvas. Dicha violación de datos permitió el acceso no autorizado a cierta información almacenada en sus sistemas. Según la investigación, los datos a los que se pudo haber accedido incluyen:

- nombres de los estudiantes,
- direcciones de correo electrónico,
- números de identificación de los estudiantes,
- mensajes de Canvas intercambiados entre usuarios.

Hasta el momento, la investigación no indica que se hayan visto involucrados contraseñas, fechas de nacimiento, identificadores gubernamentales o información financiera.

El Distrito 200 se toma muy en serio la seguridad de los datos, y nuestro Departamento de Tecnología cuenta con medidas implementadas para salvaguardar nuestros sistemas. Algunas de estas medidas incluyen:

- Hacer cumplir la autenticación de dos factores y exigir a todos los miembros del personal que verifiquen su identidad mediante un segundo factor, como una clave de seguridad o la autenticación por mensaje de texto, para acceder a su cuenta de red y a otras aplicaciones críticas.
- Restringir la capacidad de los estudiantes para enviar o recibir correos electrónicos de cualquier persona ajena al Distrito 200.
- Utilizar las mejores prácticas de seguridad basadas en niveles de acceso, así como controles internos que restringen quién tiene derechos para ver, agregar/eliminar o editar información.
- Emplear una gestión de accesos automatizada para revocar el acceso a los empleados que dejan el distrito o cambian de puesto.
- Seguir las mejores prácticas de ciberseguridad, lo que incluye actualizaciones periódicas, políticas de contraseñas robustas y la supervisión de los sistemas para prevenir el acceso no autorizado.
- Restringir y deshabilitar el acceso remoto de soporte técnico para mitigar los riesgos derivados de sistemas de terceros, con el fin de protegerse contra incidentes como este.
- Consultar con expertos federales, estatales y privados en ciberseguridad para revisar y mejorar nuestra postura de seguridad cibernética.

Queremos asegurarles que la protección de los datos de nuestros estudiantes sigue siendo nuestra máxima prioridad. Si tienen alguna pregunta sobre este incidente o inquietudes generales con respecto a Canvas o a los datos de los estudiantes, por favor comuníquense con nuestro Departamento de Tecnología a través de la dirección datasupport@wcusd200.org.