PowerSchool Cybersecurity Incident Update:

As we've looked further into the extent of PowerSchool's cybersecurity incident and its impact on Parkland there is good news and bad news. The good news is that as far as we and PowerSchool can tell:

- The following types of data were **not** accessed
  - Student profile photos
  - Computer usernames or passwords
  - Social insurance number (we do not collect the SIN for students)
  - Birth certificates or other documents associated with Parkland students
  - Staff data doesn't seem to have been accessed in our case
- PowerSchool has gone to considerable lengths to address this situation and has increased their level of security to protect against future attacks.

The bad news is that as far as we and PowerSchool can tell:

- The following types of student data were accessed
  - First name
  - Last name
  - Date of birth
  - Home/mailing address
  - Parent/Guardian contact information
  - The table that was accessed has data going back to when we started using PowerSchool (2012-2013)

In many ways, given that this was a data breach on PowerSchool's side, and they are already taking action to increase their level of security there isn't much we can do to address the vulnerabilities this incident exposes. There has been some indication that PowerSchool will provide identity protection and credit monitoring to affected students and staff. Further details on that will be shared when PowerSchool has set it up.

There are some general practices that can be followed to help protect yourself from identity theft that are a good idea regardless:

- Review email and social media accounts for unusual activity.
- Regularly update passwords for all accounts, especially if the same password has been used elsewhere.
- Use strong, unique passwords for each account, and consider a password manager for added security.
- Wherever possible, add an extra layer of security by enabling 2-factor authentication.
- Watch for phishing attempts. Look for suspicious emails, calls, or messages pretending to be from legitimate organizations. Do not click on unfamiliar links or share personal information.

These recommendations come from St. Albert Public Schools response to this incident. Please find a link to their website as well as Edmonton Catholic School Division's response for some additional information on this incident. Not all of it will apply exactly but their responses are quite thorough.
PowerSchool Cybersecurity Incident | St. Albert Public Schools
PowerSchool Cybersecurity Incident - Edmonton Catholic Schools
Additionally PowerSchool is maintaining a webpage with information on this incident:
https://www.powerschool.com/security/sis-incident/