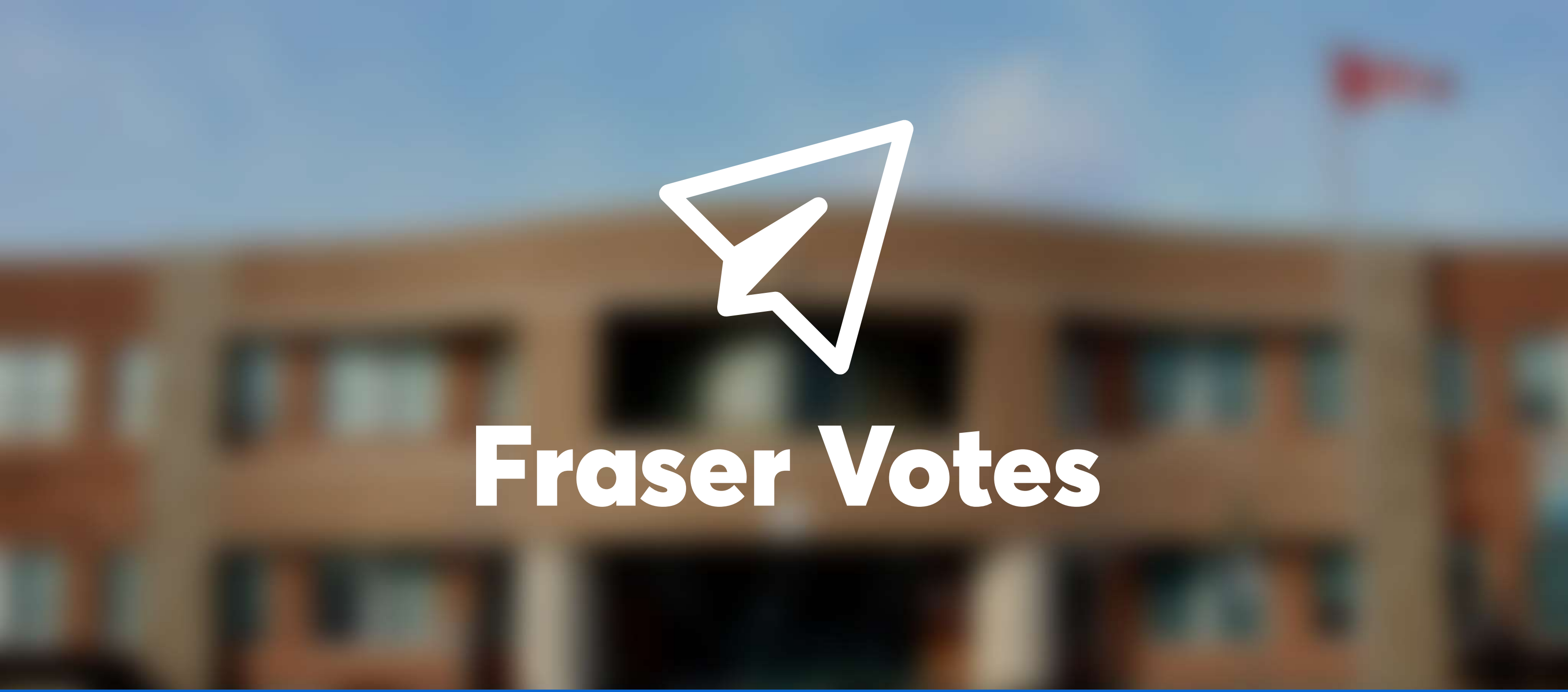
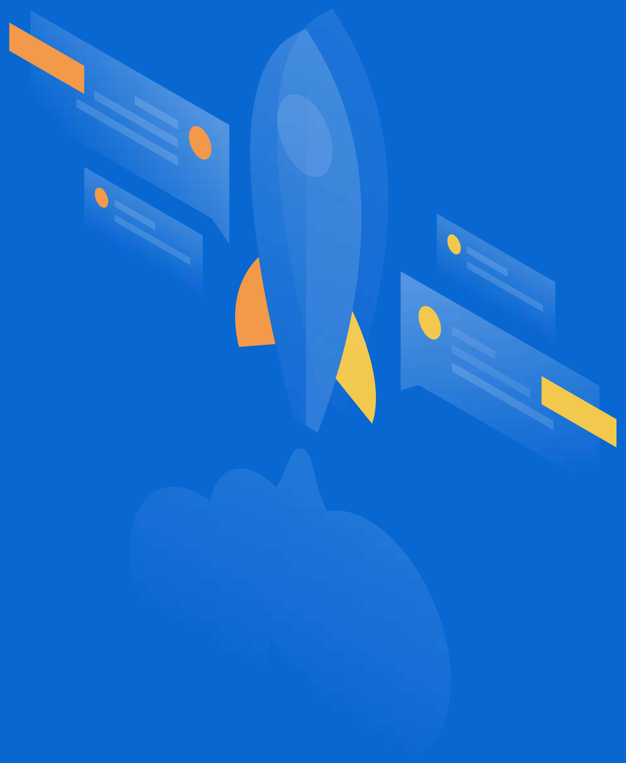


Fraser Votes

By students, for students

With elections looming and students at home, Fraser Votes is the easy-to-use, private, secure digital election management system.

The simple solution



All-in-one platform for campaigning, voting, and reporting results.

If you need help, we'll be there every step along the way to support you and implement custom features.

Transparent voting

All ballots are fully anonymized before ever leaving the browser.

Beyond simple compliance with privacy laws: we use no third-party tracking cookies.

Extreme security

Seamless integration with existing authentication providers to verify voters.

Protected by 2048-bit RSA encryption, ballots are as secure as government secrets. The key never leaves administrators' computers.

Fraser Votes. Free for Peel Schools.

Made with ☕ by David Li, Jason Huang & James Ah Yong

Fraser Votes Technical Paper

DAVID LI, JASON HUANG & JAMES AH YONG

Introduction

This paper contains an outline of how Fraser Votes is structured and how it serves as an effective digital election management solution. It is designed for readers with a basic knowledge of the relevant technologies. However, it should be understandable by those who do not have a technical background.

We will begin by giving an outline of features within Fraser Votes. We will then provide an overview of the technologies used in the creation of Fraser Votes, why they were chosen, and how they align with the goals of the project. All code is open source and available under the GitHub organization Fraser-Votes.

Features

Fraser Votes is a full election management solution from campaigning to reporting results. The following list is not exhaustive, and we are available to create custom features at individual schools' requests.

- Restricting access to specific, voting-eligible students identified by student number
- End-to-end encrypted voting
- Candidate pages with images, short statements, embedded videos, and links to social media profiles
- Delegate customization of candidates and positions to "admin" students or teachers
- Live analytics of active users, pageviews, and ballots cast
- Counting and reporting results of the election

Our team can provide support throughout the process to ensure a smooth election.

Technology Stack

Fraser Votes is a webapp built with Gatsby and React. Continuous development/integration is performed through GitHub Actions which deploys to Firebase.

Live analytics are powered by Plausible. Plausible, unlike similar analytics solutions, is a privacy-first product that does not use third-party tracking cookies.

Server infrastructure is provided by Firebase. Firebase is an app development platform created by Google which leverages Google's worldwide server infrastructure. Even though Fraser Votes is hosted on Google's servers, they do not access Fraser Votes data.

Firebase provides three services used by Fraser Votes: hosting, authentication, and databases. Hosting is the delivery of the website files from the server to users. Authentication is used to integrate seamlessly with the Peel District School Board's existing Google OAuth infrastructure on the pdsb.net domain to verify users' identities. Besides the student-number based identification, **Fraser Votes collects no names or otherwise personally identifiable information of voters.** The database stores (1) school-provided eligible voters (by their student number), (2) candidate profiles, and (3) encrypted ballots.

In compliance with Board policy, all data is stored in Canada. The Montreal-based northamerica-northeast1 server location is used for the storage and processing of all Fraser Votes cloud data. We use separate Firebase projects for each school to ensure data cannot cross between schools.

Voting Process

Fraser Votes is committed to facilitating private and secure elections. **All ballot data is end-to-end encrypted with PGP.** This means that nobody can read the ballots except for administrators with the election key. We also enforce SSL during the voting process so that ballots are not only secured at rest in our database but also in transit.

The key technology that powers Fraser Votes is PGP (Pretty Good Privacy). PGP is an asymmetric encryption protocol, most widely used in email. "Asymmetric" means that there are two keys: an encryption ("public") key and a decryption ("private") key. PGP is designed such that anyone with the public key can **encrypt** information but only the private key can **decrypt** it. Fraser Votes only stores ciphertext in our database.

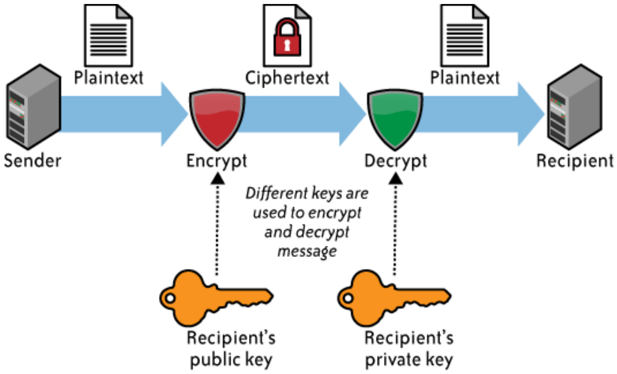


Figure 1: Asymmetric key encryption

At the start of a Fraser Votes election, administrators will create a pair of RSA 2048-bit keys using our app and save it to their computer. Key generation is performed entirely on the administrators' computer and does not use the internet; the private key never leaves the browser and the public key is sent to the database for storage.

All ballots are encrypted using the public key on voters' devices before being sent to the database. To ensure anonymity, ballots are encrypted by the individual vote (e.g. a ballot voting for president, secretary, and treasurer will create three entries in the database).

Once voting is closed, the election administrator who generated the keypair can decrypt the ballots with their private key. After all ballots are counted, the results are uploaded to the database for voters to see.

At this point, the original ballots will be deleted by the administrator.