



onefeather

Frequently Asked Questions (FAQs)

Is OneFeather Secure?

Yes. OneFeather uses multiple AWS servers in Canada (not subject to the Patriot Act) that are FIPS 140-2 compliant. We are supported by VPN and SSL terminations in AWS cloud systems using validated cryptographic modules. All OneFeather voting event websites are App Transport Security (ATS) and (SSL) TLS 1.2 compliant, ensuring all data is encrypted in transit. What this means is that all data is encrypted when transmitted and stored behind the best firewalls and data protection systems in Canada.

In addition, OneFeather systems, software, policies, and procedures are Payment Card Industry Data Security Standard (**PCI DSS**) **compliant**. Because of our exceptional data security and server reliability standards, OneFeather has an unblemished security and data protection record of accomplishment.

Finally, no data is ever stored any person's device. All our systems are cloud-based and built with technologies to the highest standards of data care and protection.

Can a Person Vote Twice?

NO – it is impossible for a person to vote twice electronically on the same voting event using OneFeather. Our systems are designed to update voter transactions, the voters list and member ledger in real time. What this means is that once you vote electronically on a voting event, you are simply not permitted to vote again.

Similarly, if you vote in person at a polling location (or by mail) and the electoral/ratification officer records your vote on OneFeather as having voted in this manner, you are not able to cast an electronic ballot for the same voting. Our systems are designed to mimic typical physical poll practices and voters list management – you only get to vote once on each voting event.

Is My Vote Anonymous & Secret?

YES! Your ballot, once cast is encrypted and stored in our electronic ballot box – no one can see it - and it can not be withdrawn, changed or otherwise tampered with. When the voting event concludes the ballot results are communicated in the aggregate to the electoral/ratification officer for final tabulation purposes. At no time is your electronic ballot ever linked to you directly – again, our designs mimic exactly what happens at a physical polling station. Once your ballot goes in the ballot box it can not be pulled out and no ballot cast can be linked back to any specific voter.

In the event of an audit or appeal – we are able to demonstrate through your digital foot-print and our authentication and verification procedures that you cast your ballot electronically, and that all ballots cast electronically are properly accounted for...just like at a physical