23 Equations App – School Room feature, Data Protection Impact Assessment

Scope of this assessment

This assessment examines the data usage of the School Room feature of the 23Equations app. Any data collected by the free part of the app, outside of the School Room feature, never leaves the device on which the app is installed and will be deleted when the app is uninstalled.

The website is for information only and 23Equations collects no data and uses no cookies. The hosting service logs access patterns to ensure standards of service. See privacy policy for more details on this.

The information collected by the app is detailed below. Also, there is a risk assessment of all possible levels of data breach and details about the protection in place to prevent and to minimise the impact of any breach.

Key points

The key points:

- Keep the Secure Key (for students' names) safe. Don't share it via email.
- Avoid using anonymous logins (required by certain app stores) to allow prompt action in case of a data breach.
- Use the minimum length acceptable for names. For example, initials for teachers and maybe first name and initial for students.
- The security of information within the app is closely linked to the already existing Email account security practices within the school.

The conclusion of the assessment is that the efforts needed to gain access to any personally identifiable information are many orders of magnitude higher than would be warranted taking into account the value of the actual information available.

The worst data breach identified would be the case of a member of staff, with admin privileges, losing control of their email account and allowing the attacker to find the Secure Key. Even in this case, they could not retrieve student email addresses but they would be able to access the names of students and link them to results of tests taken within the app.

As the tests within the app are intended for revision purposes only, the potential for harm to students is considered to be minimal.

What information is collected and why

Information	Reason	Protection
School name	For students and staff to be assured that they are logged into the right account.	Encrypted on server.
School contact email	Optional and not actually used at the moment. Intended for user to be able use to contact for help.	Optional but encrypted on the server.
Staff names	Used to identify staff to their students and other staff. It is recommended to use initials, as used in the school.	Encrypted on server. Use initials to reduce unnecessary information exposure.
Student names	Use to identify test activity to staff members. Names can be as brief as appropriate, e.g. first names with an initial.	The Secure key (created when the account is setup) is used to encrypt students' names on staff devices. Only staff members should know this key and names cannot be decoded without it. They are also encrypted again on the server. Only staff members can access student names.
All email addresses	Used to authenticate users. Allows login to be done securely without needing a password. Benefits from existing strong emphasis on email account security.	Emails are encrypted using a one way key that cannot be reversed. They are encrypted again in the database. During login, for the briefest of time, the unencrypted email, entered by the user is checked and used for sending the login pin.
Students test answer and results	These are kept so that teachers can examine and use the analysis tools built into the app to monitor and plan for progressing students learning.	There are several layers of encryption protecting the identity of test takers. The answers may be analysed statistically to help improve the service for all users.[1] No identifiable data will be made public.

[1]Planned analysis includes identifying the most common equations used in revision, identifying equations where test scores are lower than average, investigating the most effective number of questions in a test and, in the future, investigating training of neural-networks to make good recommendations of questions based on previous performance. Some very general results of this analysis may useful to share with teachers. No identifiable data will be made public.

Accessing and revoking data

All data relating to a particular student is visible to them when they are logged in to the app. Login only requires their school email address. All data held on the school is also visible to staff (with and without admin access).

Schools can request to have all or certain parts of the data wiped from the database. Students can also request to have their data removed. Both will be subject to appropriate authentication, the easiest of which is via the email addresses used in the app.

It is planned to make these features more accessible and streamlined once the app is launched and the amount of data increases.

OpenId Connect ("Sign in with Microsoft/Google/Apple")

The ability to log in using the email service providers directly instead of relying on send a pin via email has been added to all versions of the app (device based and online). This method is as secure, if not more so, as the pin method. No record of the email address is retained at all on our and the only other party involved is the external provider (Microsoft, Google or Apple). The readable form of the email address is the only piece of data retrieved by the app or servers and once this has been hashed, it is discarded. No names or any other data is requested. Also, it should be noted, to be allowed to use this service, 23 Equations had to provide cross-checked information to verify our business. The app name will be clearly displayed during the sign in process.

Risk Assessment

Summary

As detailed in the risk assessment, these are the key points:

- Gaining access to a user's email address is the most likely way for an attacker to gain access to data. This is deliberately and is mitigated by the fact that **email account security awareness is already a significant part of school life** for both students and staff.
- The Secure Key, used to encrypt student names, is the second critical piece of information. Share cautiously only with staff who need this information. It is only useful if someone also has access to a staff member's email account. **Do not send the secure key by email!** Doing so would mean email access alone would allow access to student data.
- Teacher names are not encrypted using the Secure Key so that students can identify the teacher without needing anything other than their email address. **Using initials instead of full names for staff** would be best practice.
- Only staff members who are given account admin access can changes to personal data, such as names and email address. **This level of access should be restricted to as small a group as possible** to lower the risk of a significant breach of security.

- Restoring protection to compromised accounts is more difficult when the account is anonymous. **Supply a contact address during account setup and opt for email-based authentication** of the admin account.

Risk	Impact	Mitigation
Malicious attacker who: • Knows a student or staff members account	Can pin numbers to be sent to the email account causing a nuisance	• The server keeps track of the number and frequency of pin requests and blocks new request after a small number. • If necessary, **staff members with admin access can block new account logins which will prevent any such attack**.
Malicious attacker with: • Access to a student's email account	Access to that student's answers and scores in revision tests taken on the app. Ability to answer incomplete tests instead of the student.	• Normal email account security as promoted by the school. • **Staff members with admin access can revoke and block any logins** for the student's account preventing further access by the attacker. • **Tests should be checked as answers during the attack may not be from the student.**
Malicious attacker with: • Access to staff member's email account (but <u>no admin access and no secure key</u>)	Logging in to the app will be possible but data download will not be possible without the key	• Normal email account security prevents this attack. • No security is breached. • Make sure **the secure key is kept secret and never shared via email.** • If there is evidence that the app has been accessed (e.g. a pin code email from 23Equations), it is possible for all current logins for that account to be revoked. The attacker would no longer have access to the account without again using the staff member's email account. Conclusion: As long as the key is kept secure, even access to a staff members account will not grant access to the key. Email account security is already a normal part of school life and this build on that. Revoke logins of the compromised account to restore security.

Malicious attacker with: • Access to staff member's email account (but no admin access) • Access to the secure key for this school account	Access to names and scores for tests taken through the app by students within the school. Ability to set tests for assigned groups.	• Normal email account security prevents this attack. • Make sure **the secure key is kept secret and never shared via email.** • If there is evidence that the app has been accessed (e.g. a pin code email from 23Equations), it is possible for all current logins for that account to be revoked. The attacker would no longer have access to the account without again using the staff member's email account. • No email addresses (other than the account email and school contact email) are visible even at this level of access. • Names cannot be changed without admin access. **Limit the number of staff members with this level of access**. • Any tests which have been set by that staff member can be revoked. • **Test names should be checked and changed as these are the only significant way to benefit from compromising the account**. Conclusion: As long as the key is kept secure, even access to a staff members account will not grant access to the key. Email account security is already a normal part of school life and this build on that.
Malicious attacker with: • Access to staff member's email account • Staff member has admin access • Access to the secure key for this school account	Access to names and scores for tests taken through the app by students within the school. **Ability to change names and emails of students and staff.**	• The secure key should be only be shared verbally and not via email so there are two independent methods of authentication. • At least one other member of staff with admin access who can log out the staff member, requiring access to the email account to login again. • Although more than one admin is desirable to recover control of the account, giving admin access to everyone would increase the likelihood of this kind of attack. • Even with this level off access, no email addresses are visible (other than school contact email and the staff member's own address) but email addresses could be changed. • **This is the worst level of account compromise**. Please seek advice from support if this happens. • **Note**: if **anonymous account login is used (IOS) it will be significantly more difficult to deal with this issue** because it is very difficult to verify identity. Conclusion: Members of staff are expected to protect access to their email accounts. In addition to this, **the secure key should be kept secret and not shared via email**. Have **more than one account admins but only one or two more**.

Malicious attack with: • Data stolen from a Staff member's device via malicious software	Access to local database	The decrypted versions of student names are not stored in the local database on the device. Access to the local database file on its own would not grant access to any student Personal Data. The Encryption Key and knowledge of how it is used would be required. All emails are safe for reasons describe above. Staff names are not encrypted and could be visible, another reason that initials only should be used for staff names. Test data is also not encrypted. Login credentials are stored in the device's secure area NOT in the local database so would safe. Normal procedures which would be expected to be in place to secure devices against Personal Data loss should prevent this attack mode. If a successful attack takes place, the remaining layers of encryption make further access attempts unreasonably demanding given the nature of data which would be obtained.
Malicious attack with: • Access to 23Equations database	Access to encrypted data	• The database is protected by secure credentials storage and restricted IP access. • **Contact email addresses would be used** to inform users in the event of this happening (**unless the account holder opted out** of supplying an email address during sign up). • All names of schools and teachers are encrypted before being stored in the database. The key is not accessible from the database. • All student names are encrypted on staff device and further encrypted before being stored in the database. It is not practically possible to decrypt these names. • All email addresses (except school contact email) are hashed using a one-way function then further encrypted. It is not possible to decrypt these names to obtain email addresses. With access to the database only, an attacker would be unable to identify students even with a known email address. Conclusion: There is no known way for an attacker to access identifiable data of unknown students via the servers. Further, the effort required to access a student's test results via a known email address is unreasonably beyond the value of the information that would be obtained.

Malicious access to all 23Equations Azure service (database and server)	Access to encrypted data. Access to server functions.	• Mandatory Two-factor identification and restricted IP access to server accounts restrict access to database and the servers. • **Contact email addresses would be used to inform users** in the event of this happening (**unless the account holder opted out** of supplying an email address during sign up). • Secure storage of access and encryption keys. • All names of schools and teachers are encrypted before being stored in the database. Significant reverse engineering would be required to access this information. • All student names are encrypted on device of the school staff member who is the account admin before even reaching the servers. The encryption key is only known to staff of the school. They are further encrypted before being stored in the database. It is not practically possible to decrypt these names. • All email addresses (except school contact email) are hashed using a one-way function then encrypted once more. It is not possible to decrypt these names to obtain email addresses. With significant reverse engineering of the server code, it may be possible to match a known email address against records in the database and thereby identify tests which were taken by that individual. Conclusion: there is no known way for an attacker to access identifiable data of unknown students via the servers. Further, the effort required to access a student's test results via a known email address is unreasonably beyond the value of the information that would be obtained. Similarly, names of staff members would require significant reverse engineering. To further degrade the benefits of this, it is **suggested that staff names are entered as initials only.**