# Security Considerations During Development

The Dunfermline Men’s Shed is an organisation that exists to provide a safe and healthy space for its members to gather, socialise, work together and take part in a number of different activities and interests. The organisation does not engage in political activity nor holds any beliefs that are commonly interpreted as inflammatory/extreme and as such is extremely unlikely to have a heightened risk of being targeted above and beyond the traditional threats of existing on the modern internet.

The main assets to be considered in the context of security for this application development project are the members personal information and the application itself.

As members personal data will be stored on the application/database this brings GDPR into play, all reasonable steps must be taken during the development of the application to ensure the security, integrity and availability of the members personal details at all times.

Member information should be encrypted with a suitable encryption algorithm in all data states at rest, in-transit and where possible in-use as well. An appropriate cipher suite should be used for client-application to server communications.

Passwords should be stored using a secure hashing algorithm (not md5 or sha-1) and not stored in plain-text.

During development of the application there are particular areas to focus on with regards to keeping the application secure.

Due to a SQL database/web front-end setup strict input-validation will be key, enforcing strict input-validation at both the client-side of the application and server-side will reduce many risks from command-injection, buffer-overflow attacks and the old but still possible SQL injection attacks.

Development of the application should include functionality to redirect incoming HTTP traffic to an HTTPS secure connection, this should be done automatically behind the scenes to provide the security benefits without confusing or placing the responsibility onto the user.

Appropriate secure headers should be used in order to mitigate the risks from cross-site scripting attacks and clickjacking.

A password policy should be enforced for the users on the app so that they are using relatively secure passwords for their accounts for example minimum of 8-chars with a mix of upper and lower-case and/or special characters. Rate-limiting the amount of unsuccessful login attempts to 3-5 is recommended as well, this is to reduce the risks from brute-force/dictionary attacks against user accounts.