Purpose

The aim of this document is to give basic guidance to prospective authors of applications for mobile devices such as smartphones and tablets.

Guidance

1. **Address a distinct problem** - focus on a single problem or subject and avoid bundling unrelated functions together. It should be possible to describe the application succinctly in a short paragraph or sentence.
2. **Design for understandability** – ensure the app is understandable in its own right without undue dependencies on other applications or systems.
3. **Keep it simple** – do the simplest thing that works and avoid unnecessary complexity.
4. **Multiplatform or native development** – consider carefully whether to use a platform-specific native code development kit or a multiplatform development environment based on HTML5 and web technology. A multiplatform approach gives wider coverage, greater flexibility and faster time to market while native code may be more appropriate if your app requires high performance or access to physical device features that are not yet available via HTML5.
5. **Feasibility** – the choice of development tools, the target platforms and the type of application also depend on the development skills available to you. The IT Innovation Centre may be able to put you in contact with others who may have the skills that you are currently lacking.
6. **Accessibility** – consider the needs of potential users with poor vision, hearing, manual dexterity etc.
7. **Governance** – if you want to use the University’s name or logo, the IT Innovation Centre will help submit your app to the University Mobile Steering Group (UMSG) for approval.

Tools

The cross-platform development tools preferred by IT Services for University projects are:

- **Cordova/Phonegap** – PhoneGap is a free distribution of open source Apache Cordova which allows app development using HTML5, Javascript and CSS. See [http://phonegap.com](http://phonegap.com) or a commercial cloud-based version at [http://www.icenium.com](http://www.icenium.com).


However these are not necessarily the most appropriate in all cases and you should select the tools you feel are best suited to your project. Contact the IT Innovation Centre for advice, or help with licensing.

Security Considerations

Most of this will likely not apply but it is as well to be aware of it just in case.

The presence of confidential information on mobile devices represents a major vulnerability and a risk if the device falls into the wrong hands. Therefore precautions need to be taken to protect the data whether it is contained in emails, documents or files. Confidential covers:

- Personal details that fall within the scope of the Data Protection Act including **race or ethnic origin, political or religious convictions or similar beliefs, trade union membership, physical and mental health, sexual orientation and activity, and criminal allegations, proceedings or convictions**.
- Financial data, bank account numbers, credit card details etc.
- Intellectual property such as sensitive unpublished research, trade secrets etc.
- Contracts, commercial information provided in confidence and anything that might put at risk the University’s reputation or legitimate interests.

Confidential data must be protected as follows:

1. **Authenticate** – insist on entry of a password or code before giving access to anything confidential. Smartphone unlock codes are generally not sufficient because they are notoriously easy to break.
2. **Encrypt** – to a level that complies with the University’s Cryptography Standard (AES 256):
   - access to confidential data via the Internet or campus network using HTTPS or mobile VPN.
   - stored confidential data whether in the form of emails, documents, files etc.
**Guidelines – Mobile Apps**

**Glossary**

- **AES 256**
  Advanced Encryption Standard (AES) with 256 bit keys, the University’s current standard.

- **CSS**
  Cascading Style Sheets – controls the look and feel of web pages.

- **HTML5**
  The latest incarnation of Hyper Text Markup Language is suited to low powered devices such as smartphones and incorporates many new features such as access to location services, 3d graphics etc.

- **HTTPS**

- **JavaScript**
  Java-like scripting language used for web-site application development.

- **Ruby**
  General purpose object oriented programming language that combines Perl like syntax with Smalltalk-like features.

- **UMSG**
  University Mobile application Steering Group – University IT governance committee responsible for mobile device apps.

- **VPN**
  Virtual Private Networking – an encrypted communications ‘tunnel’ between two end points on the Internet.

**Information**

For further information, refer to:

- University Mobile App Steering Group (UMSG) – [http://intranet.birmingham.ac.uk/mobileappsgroup](http://intranet.birmingham.ac.uk/mobileappsgroup)
- Help with submitting mobile apps – [http://intranet.birmingham.ac.uk/it/innovation](http://intranet.birmingham.ac.uk/it/innovation).