Mobile App Developments Policy

Version Control

Version number	Date published	Changes from previous version
Version 1	November 2020	First version
Version 2	July 2025	New structure and processes in line with requirements in current operating environment

Contents

Background

The Information Services Directorate (ISD) manages the University's Mobile App Service. This service is responsible for the development, delivery, hosting, advice and guidance of Mobile Apps for the University of Strathclyde, primarily released through the University's app stores.

The Mobile App Service is responsible for strategic decision-making in respect of all University mobile apps – existing and proposed - with the support of the Information Services Management Team and in line with Strathclyde 2030 and the University's Digital Strategy. Decisions will always be made in the best interests of the University, especially in respect of University Values, consistent student experience, cyber security, app store management, and uptime of critical student services.

This Mobile App Developments Policy outlines key principles and processes for Mobile App development, delivery, collaborations (internal and external), and provides a framework for the application of these.

Our Mobile App Developments Policy aims to follow a continuous collaboration and co-creation approach, putting our users, particularly our student customers, at the heart of our technologies, development and delivery. As a leading technological University, innovative and collaborative ideas and approaches are always at the forefront of all we do. **The Mobile App Service welcomes debate, bold and innovative ideas and open discussion** and is continually reviewed and refined in line with that ethos.

Scope

This policy applies to all staff and students. For the purposes of this policy, a mobile app (also referred to as 'app') is a software application developed specifically for use on devices such as smartphones and tablets and distributed through mobile app stores such as Apple's App Store and Google's Play Store.

The scope of this policy includes all mobile apps released through the University's app stores. It includes the following types of apps:

- **The core, corporate app for students and staff:** StrathApp
- **Third-party apps:** purchased by the University, usually on a licensed basis, built and maintained by a third-party supplier
- **Research apps:** built as the outputs of academic research
- **Teaching apps:** built by students as part of their academic studies
- **Entrepreneurship apps:** built by students or staff in support of societies, interest groups or for commercial purposes

Apple School Manager/Management of Apple mobile devices

Apple School Manager can be used for the management of University-owned Apple devices, e.g. for the management of Macs or iPhones. For enquiries about Apple School Manager, please contact the End User Computing team via the IT Helpdesk.

Principles for all University Mobile Apps

1. Services are **User First**
2. Services are developed through **Continuous Collaboration** between all stakeholders, ensuring clear, coherent user journeys across all University digital platforms
3. Apps are provided in **both the Apple App Store and Google Play Store**, at a minimum
4. Services are **Brand Compliant** and **Accessible** to all users
5. Services are **Cyber Secure**
6. Data transfers are from trusted data sources via the **Corporate Integration Hub**
7. Services are compliant with legislation and regulations in areas such as **Data Protection, PCI Compliance, Marketing, Digital Accessibility, Procurement** and **App Store Licensing**

Responsibilities

Mobile App Oversight Working Group (MAOWG) is responsible for:

- Liaising closely and proactively with the Mobile App Service
- Strategic decision making for all apps that require hosting in the University's App Stores
- Prioritisation of available App Store distribution certificates (these are limited in number – see Third Party App section of this policy)
- Making recommendations to DCSC/ISC for approval of business cases involving mobile apps (see Third Party App section of this policy)
- Providing advice and guidance to the Mobile App Service in cases of dispute, or lack of compliance with this policy or the **Standards for Third Party Access to Stores**

The Mobile App Service is responsible for:

- University Mobile App Strategy, Policy and Standards
- Day-to-day service management and support for the University's core, corporate student and staff app, including:
  - Management and scheduling of content
  - Direct student messaging protocols (in partnership with Student Experience, Strath Union etc.)
  - VLE alignment (in partnership with Education Enhancement)

- Account management of the University's App Stores (currently Apple and Android): maintaining compliant accounts and authorising access for third parties (outwith the StrathApp team) via formal approval routes
- Advice & guidance on mobile app technologies and tools

Individuals and teams (staff and students) developing apps or purchasing third-party apps are responsible for:
- Ensuring all parties adhere to all relevant policies and guidance, especially the Mobile App Service's **Standards for Third Party Access to Stores**
- Identifying and following the correct approval processes for the proposal and implementation of new apps (see Management Policies section below)
- Liaising closely and proactively with the Mobile App Service at all times

Management Policies

Core, Corporate App for Students and Staff

StrathApp is the University's core, corporate student and staff app. It hosts a range of services and serves as a window to data held in other University systems - providing real-time, on-the-go information to its users. StrathApp is built and maintained in-house by the Mobile App Service. The development of new services is user-led, based on consultation and collaboration with students and staff.

Suggestions or proposals for new services - and other forms of feedback - are always welcome. Please contact strathapp@strath.ac.uk.

Third-Party Apps

StrathApp is the University's corporate student and staff app; the 'One Corporate App' approach has been extremely successful to date. It is recognised, however, that there are circumstances in which a third-party app may be required, in order to provide specific functionality that does not already exist in StrathApp and which does not more appropriately belong within the University's one corporate app approach.

Where a third-party app is proposed, **prior to any procurement**, a business case will need to be submitted to, and approved by, the Digital Strategy Programme Board, to ensure appropriate governance and funding. Resourcing for third-party apps should be determined by the Mobile App Service and defined separately from the procurement and implementation of companion or parent IT systems. Please contact strathapp@strath.ac.uk for advice at the earliest opportunity. **If a third-party**

app has been procured without a business case, there is no guarantee it can be released through the University app stores.

Key factors are:

1. **Standards:** Any procurement and implementation of third-party apps will be subject to strict compliance with a range of standards in order to maintain the security, accessibility, quality and reputation of all apps provided through the University of Strathclyde's app store accounts. These standards are detailed in the **Standards for Third-Party Mobile App Developers and Access to University Mobile App Stores document**.

2. **App Store Distribution Certificates:** the Apple App Store limits the number of distribution certificates a single organisation can have. One certificate will always be solely allocated to StrathApp. Any additional approved apps will therefore have to be prioritised in the context of the remaining certificates available. DCSC/ISC will determine which apps will be granted use of the App Store certificates in the University's stores, based on recommendations from the Mobile App Oversight Working Group.

3. **Payments through apps:** a proposed app which would take payments in any form requires liaison with the Cyber Security compliance team and the Finance systems team at the very earliest stages of consideration to ensure PCI-DSS compliance is achieved to the satisfaction of the University and the payment service provide can provide secure data for accounting on the Finance system.

4. **Implementation support:** all third-party access to the University's app stores is limited and closely monitored for security reasons. Therefore, implementation and ongoing updates must be facilitated by the Mobile App Service at pre-planned and mutually agreed times. It is expected that the business owner of the third-party app (the University area/team that has proposed it) will proactively manage all communications with their supplier, including arranging their access to the University's app stores in line with the notice periods defined in the **Standards for Third-Party Mobile App Developers and Access to University Mobile App Stores** document.

5. **Business as usual support:** it is expected that the business owner of the third-party app will lead in closely and proactively managing both the supplier and ongoing updates to their app, ensuring close co-ordination with the Mobile App Service at all times.

Third-party app proposal process

1. Initial proposal submitted through the Digital Ideas form, managed by the University's Programme Management Office (PMO)
2. The PMO's Digital Ideas Group provides the proposer with this policy and the **Standards for Third-Party Mobile App Developers and Access to University Mobile App Stores**
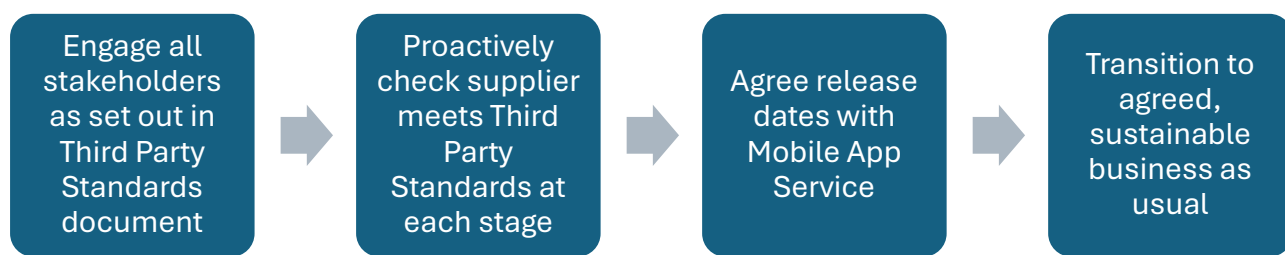
document. The standards document must be thoroughly reviewed and the relevant teams must be engaged with ahead of, and in support of, the next step - the business case.

3. The proposer writes a business case, liaising with the Mobile App Service to determine implementation and resourcing requirements. It is important to ensure the business case includes the resourcing requested by the Mobile App Service (and other teams as detailed in the Standards for Third-Party Mobile App Developers and Access to University Mobile App Stores document), including ongoing, business-as-usual resource.

4. Mobile App Oversight Working Group (MAOWG, a sub-group of DCSC) convenes to review the business case and consider key factors including timescales, resources and use of app store certificates. The MAOWG will make recommendations to the approving groups – DCSC and ISC.

5. Approval of business case from DCSC/ISC, including agreed timelines and resources.

| Iniital proposal submitted to Digital Ideas form | → | Standards for Third-Party Apps given to proposer for review | → | Proposer writes business case with input from Mobile App Service | → | Mobile App Oversight Working Group recommends approval or not | → | Approval of business case from DCSC/ISC |

Third-party app implementation process

1. Before procurement commences, engage with teams such as Cyber Security, Information Governance, Equality and Branding to ensure all standards and compliance points are documented in clear quote or tender requirements (refer to the **Standards for Third-Party Mobile App Developers and Access to University Mobile App Stores** document for further details).

2. Actively work with the chosen supplier to ensure all standards are delivered both pre and post procurement.

3. Identify appropriate release dates as early as possible by consulting with the Mobile App Service who will determine which dates are compatible with all other University apps and their release schedules.

4. Transition to a sustainable, resourced business-as-usual service delivery model.

Engage all stakeholders as set out in Third Party Standards document → Proactively check supplier meets Third Party Standards at each stage → Agree release dates with Mobile App Service → Transition to agreed, sustainable business as usual

Research, Teaching & Entrepreneurship Apps

App development is a fast-moving and innovative area, and we welcome a continuous collaboration and co-creation approach. However, the University's Mobile App Service is designed to support app development of core, central student services and therefore cannot, on a practical basis, support all app proposals and ideas that are brought forward.

Outlined below are the processes for some broad areas of app development across the University.

Research apps

Research apps are built as the outputs of academic research. They may be released to a closed testing group only or issued on an open release, i.e., anyone with access to the relevant app store is able to download and use the app.

In 2025, the Mobile App Service team will embark on a pilot of a small number of research apps in conjunction with the University's Computer and Information Services department. These apps will be released to a closed testing group only and will not be available to the public through the University's app stores.

Where research apps are proposed for open release through the University app stores to any member of the general public, they must follow the approval process set out in the Third-Party Mobile Apps section of this document.

Other requirements for all research apps:
- Research apps will have to share distribution certificates with other research and third-party apps.
- There must be clarity about who has successfully completed the ethics requirements. This is especially important where universities are working in partnership on the research; there must be clearly defined and documented ownership of the ethics requirements.

Teaching apps

The University's app stores are not available to students for teaching or assessment activities. Support for apps built by students as part of their academic studies must be managed solely by the academic department. For advice on creating individual developer accounts or use of the Apple and Google Play stores, please consult their official guidance.

Entrepreneurship apps

Entrepreneurship apps are apps built by students or staff in support of societies, interest groups or for commercial purposes. The Mobile App Service is underpinned by a student co-creation model and, as such, we welcome innovative ideas for app development.

Proposals for development of entrepreneurship apps that will require University central support (in terms of consultation, analysis or development), managed access to University app stores or integration with StrathApp must:

- Have a University Department sponsor
- Have approval from the Mobile App Oversight Working Group
- Have a funding route identified (to pay for resources, including the University's Mobile App Service resource)
- Be supported by a business case (see section on Third Party Apps in this document)

Appendix

Definitions

App Stores: platforms for the distribution (download by users) of mobile apps. Examples include Apple's App Store, Google's Play Store and the Microsoft Store. The administrative accounts for allow mobile apps to be provided to users through a University ownership of the University. The administrative accounts for the University's App Stores (Apple, Google and Microsoft) are owned and managed by the Mobile App Service.

DUNS number: The Dun & Bradstreet D-U-N-S Number is a unique nine-digit identifier for businesses. For the University, it is linked to the Companies House listing generated by the Privy Council. A D-U-N-S Number is used by some suppliers – including the App Stores – to identify and verify a business and is linked to firmographic data (company name, address, phone number, etc.) and corporate family relationships (headquarters, branches, subsidiaries, etc).

App Store distribution certificates: used by Apple and Google as a requirement for the distribution of apps in App Stores. These certificates are deliberately limited number and it is best practice to only share within your organisation. Some third-party suppliers mandate that they have sole use of a distribution certificate; this is also University policy for our one, corporate app. StrathApp.