



University of
Strathclyde
Glasgow



Standards for Third-Party Mobile App Developers and Access to University App Stores

Version Control

Version number	Date published	Changes from previous version
Version 1	July 2025	First version

**THE QUEEN'S
ANNIVERSARY PRIZES**
1996, 2019, 2021 & 2023
For Higher and Further Education

**UNIVERSITY
OF THE YEAR**
2012 & 2019
Times Higher Education

**UNIVERSITY
OF THE YEAR**
2024 RUNNER-UP
Daily Mail University of the Year Awards

**SCOTTISH UNIVERSITY
OF THE YEAR**
2024
Daily Mail University of the Year Awards

**EUROPEAN ENTREPRENEURIAL
UNIVERSITY OF THE YEAR**
2023
Triple E Awards

Contents

Version Control	1
Introduction	3
Definitions	4
Purpose & functionality of mobile apps	4
Use of University data in third-party mobile apps	5
Authentication	5
Compliance standards	5
Contractual relationship	5
Cyber security	6
Data protection	6
Financial & PCI compliance	7
Equality & Digital Accessibility	7
Branding	8
Third-party support: reporting and escalation of issues	8
App store standards	8
Acceptable Use of App Store Access	9
App Store Content	9
Maintaining Third-Party Apps in App Stores	9
Secure Storage of Credentials	9
Failure to meet standards	10
Granted Roles/Permissions within University App Stores	10
Apple Developer and App Store Connect	10
Google Play	10
Access Request Protocol	11
Release protocols	11
Testing	12

1. Introduction

Collaboration Services (CS) – part of IT Services at the University of Strathclyde – is responsible for StrathApp, the University’s core, corporate student app. It is also the institutional owner of the University’s Mobile App Service, as defined in the **Mobile App Developments Policy**. Therefore, CS 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 Strategy 2030. Decisions will always be made in the best interests of the University, especially in respect of University Values, cyber security, app store management, and uptime of critical student services.

Collaboration Services is responsible for StrathApp, the University’s corporate student and staff app. This ‘One Corporate App’ approach has been extremely successful to date and the team have extensive knowledge and experience upon which to continue to evolve the Service. 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. In these circumstances, it is expected that consideration, procurement and implementation of a third-party app will be progressed in accordance with the University’s **Mobile App Developments Policy**.

This document sets out the standards which must be adhered to in order to maintain the security, accessibility, quality and reputation of all mobile apps provided through the University of Strathclyde’s App Store accounts. Some of the content in this document has been drawn from the UK government’s [‘Code of practice for app store operators and app developers’](#) and its eight key principles, therefore aligning with recognised best practice in respect of security and privacy requirements; other content is passed down through statutory obligations on the University as a quasi-public sector body, alongside other University-defined requirements.



2. Definitions

The following definitions apply to this standards document:

- **University Business Partner:** the team within the University that have responsibility for requesting, purchasing and managing a third-party mobile app, including the relationship with its supplier.
- **Third-party developer:** an external supplier to the University of Strathclyde, specialising in the development of mobile apps.
- **Mobile App Service:** the institutional owner of all University mobile app services, responsible for the governance and management of the deployment of mobile apps via the University App Stores.
- **University App Stores:** the University's accounts for mobile app stores; includes Google Play, Apple's App Store and the Windows Store.
- **App:** means mobile application releasable through the University App Stores.

3. Purpose & functionality of mobile apps

Where the new mobile app will provide functionality that already exists, or partially exists, on any system within the University, it is required that user journeys be documented detailing how end users will be able to navigate both/all systems without confusion. It is expected that this work is performed in

tandem with end users well in advance of release and is also the subject of successful user acceptance testing.

4. Use of University data in third-party mobile apps

Where a third-party app requires use of University data other than that provided directly by the end user, the transfer of University data must be via the University's Integration Hub and by API. Agreement for resourcing must be established with the Integration Hub before the third-party app is procured. The amount of resource required to facilitate the work is a determination that lies with the Integration Hub not the third-party supplier. The University's Information Governance Unit will also need to be consulted ahead of procurement commencing in respect of data sharing or data processing agreements (see [section 5.3](#)).

4.1. Authentication

Where a third-party app requires use of University authentication methods such as single sign-on (SSO), resourcing for this must be established with the University's Infrastructure team before the third-party app is procured.

5. Compliance standards

All third-party suppliers, in conjunction with their University Business Partners, must **comply with the requirements in this section – and agree to ongoing adherence - before access will be granted to University's App Stores**. Many of these steps need to be completed **before procurement** is complete. It is expected that **the University Business Partner will lead the performance and delivery of these processes**, seeking support from the relevant Strathclyde teams, as set out below.

5.1. Contractual relationship

Third-party developers will be provided with access to University App Stores only where the third-party developers have a direct contractual relationship with the University for the purposes of developing and supporting mobile apps. Where there is uncertainty about what a contractual relationship covers, it is advisable to contact the [University's Procurement team](#).

In all cases, access to the University App Stores will be by request only and for a limited time window agreed in advance (see [section 10](#)).

5.2. Cyber security

Cyber security requirements must be part of mandatory prerequisites presented during the procurement process. Apps with insufficient cyber security measures will not be permitted to access the University's App Stores even if the purchase has been completed.

The UK government's ['Code of practice for app store operators and app developers'](#) and its eight key principles focused on security and privacy requirements forms part of the basis for these standards. It is expected that third-party suppliers will review the following principles from the code and either confirm compliance or report any instances of non-compliance:

- [Principle 2: Ensure apps adhere to baseline security and privacy requirements](#) – all parts
- [Principle 3: Implement a vulnerability disclosure process](#) – 3.1 only
- [Principle 4: Keep apps updated to protect users](#) – 4.1 and 4.2 only

The University also has its own cyber security policies and requirements which the app must align with. This may include the app, company and process being risk assessed, and the app subjected to vulnerability scanning and penetration testing.

Any breaches of cyber security must be immediately notified to the University to allow the University to instigate their Cyber Incident Response Plan. In the event of a cyber-attack, the Mobile App Service may remove all access to University App Stores without notice and reserves the right to determine when access is restored.

5.3. Data protection

In line with University requirements, a Data Protection Impact Assessment (DPIA) must be completed by the University Business Partner before a procurement exercise can proceed. Further information can be found on [the University's Data Protection SharePoint pages](#). The DPIA must be approved by the Information Governance Unit as part of the procurement process and then regularly updated as further detail is available during and post-implementation. As part of the DPIA process, it is expected that a data sharing or data processing agreement will be in place - and approved by IGU - as required.

To fulfil app store requirements and provide data protection compliance, a privacy notice is also required for each app. The University's Information Governance Unit (IGU) has [produced useful information about the requirements of a privacy notice](#) and what types of processing are already covered by the University's central privacy notices. Further advice and guidance can be sought directly from the IGU. All requirements from [sections 5.3 and 5.4 of the 'Code of practice for app store operators and app developers'](#) should be covered in the privacy statement, as a minimum. The

production of the privacy notice and its approval by the IGU is the responsibility of the University Business Partner.

Third-party suppliers must alert the University as soon as they become aware of a data breach involving personal data.

5.4. Financial & PCI compliance

Where it is expected, either on initial release or in a future release, that an app is to be purchased from the University App Stores (a 'paid-for app') or that an app will collect payments from the end user, the University Business Partner must make this known early in the process of considering a new app. Finance and PCI compliance requirements must be part of mandatory prerequisites presented during the procurement process and these requirements must be written in collaboration with the PCI Compliance, Finance and Financial Systems teams at the University.

It is also expected that the University Business Partner and third-party supplier will thoroughly research and comply with any additional app store requirements resulting from these payments. For example, in relation to tax declarations or the requirement to pay the app stores a percentage of the proceeds of sale.

Paid-for apps or apps which collect payments from the end user which do not comply with all PCI and Finance requirements will not be permitted to access the University's App Stores even if the purchase has been completed.

5.5. Equality & Digital Accessibility

In line with University statutory obligations, it is expected that an Equality Impact Assessment (EIA) is completed by the University Business Partner early in the process of considering a new app. Similarly to a DPIA, it will need to be updated as the implementation progresses to reflect the practical implementation of the product. Further information can be found on [the University's Equality and Diversity SharePoint pages](#).

The University has a [statutory obligation to provide accessible digital content](#), including mobile app content. Therefore, it is expected that all apps released from the University App Stores meet the WCAG 2.2 AA standard. In addition, it is required that every app displays an [accessibility statement](#) within the relevant app store and/or app. The accessibility statement itself must be digitally accessible.

5.6. Branding

All apps released from University App Stores must adhere to the [University's branding guidelines](#). Assistance on the correct application of branding to a third-party app may be sought from the University's web team.

The app stores require that each app has a name and a logo appropriate for the stores. The University Business Partner must ensure these are approved by the University's Marketing & Communications team. The logo must be of a design and quality that enables it to display as expected on a range of screen sizes, and which makes it easily distinguished from other apps released via the University App Stores.

5.7. Third-party support: reporting and escalation of issues

University Business Partners must ensure that third-party apps have a suitable support process for users, usually defined by a Service Level Agreement (SLA) with the third-party supplier. As a minimum, it is expected that, in terms of support, the SLA sets out:

- Expected app uptime
- Process for notifying users about planned and unplanned downtime
- Process for raising issues experienced by end users
- Target response and resolution times for issues raised
- Agreed named contacts at the University with whom the third-party supplier will liaise over issues raised

In addition, it is required that the University Business Partner write a Standard Operating Procedure (SOP) for the University's IT Helpdesk to enable the IT Helpdesk to accurately and efficiently route enquiries regarding the third-party app. The SOP must be provided to the IT Helpdesk at least four weeks in advance of the app's release. It may also be necessary for the IT Helpdesk to be provided with a demo to better enable them to understand what the end users they support may be experiencing.

6. App store standards

The University of Strathclyde requires all third-party developers to abide by the relevant terms of service for the app stores they will access on the University's behalf:

- The Google Play store's terms are detailed in their [Developer Distribution Agreement](#).
- The Apple App Store's terms are detailed in their [general terms page](#) and their [Apple Developer Program License Agreement](#).

7. Acceptable Use of App Store Access

Access to the University's App Stores will be granted to third-party developers to facilitate the following tasks only, which we recognise are required to manage apps on behalf of the University.

- Create new versions of the third-party's app
- Manage certificates and provisioning profiles relating to the third-party's app
- Manage internal testers for the third-party's app
- Upload new builds of the third-party's app for internal testing
- Upload new builds of the third-party's app for distribution
- Submit and publish builds of the third-party's app
- Update app store listings for the third-party's app

7.1. App Store Content

All third-party developers must regularly review the app store listings for their app, keeping any content (text, images and links) and security and privacy measures up-to-date, in line with the cyber security requirements set out in Principle 4 of the UK government's ['Code of practice for app store operators and app developers'](#) (see [section 5.2](#) of this document).

7.2. Maintaining Third-Party Apps in App Stores

Where the Mobile App Service become aware of issues in the University App Stores related to third-party apps, the University Business Partner will be informed. It is the University Business Partner's responsibility to alert their third-party supplier and oversee the timely identification and resolution of the issue. Where necessary, the University Business Partner can also request the assistance of the Mobile App Service to assist with the resolution of the issue. Oversight of resolution and communication between all parties remains the responsibility of the University Business Partner.

7.3. Secure Storage of Credentials

Third-party developers will be responsible for securing the Developer or Service accounts they use to maintain Apps they are responsible for within the App Stores.

- Account credentials must be kept secure, using a password manager with strong encryption.
- Accounts should have MFA enabled to provide an additional layer of security.
- Accounts must be associated with a main account holder that the Mobile App Service can contact should issues arise, not a generic email address.
- Any lapse in the security arrangements for the account credentials of the App Stores must be reported to the Mobile App Service immediately.

8. Failure to meet standards

In the following circumstances, the Mobile App Service reserves the right to immediately withdraw third-party access to the University's App Stores:

- Cyber security attack or breach
- Significant issues with the quality of the app
- Failure to meet compliance standards
- Failure to comply with the relevant app store's terms of service
- Failure to adhere to acceptable use of the University's App Stores
- The app is causing a negative impact on the approval, distribution, security or function of other apps offered by the University of Strathclyde

9. Granted Roles/Permissions within University App Stores

The Mobile App Service holds the highest level of permissions in all University App Stores and will grant the permissions set out below to third-party suppliers, subject to ongoing compliance with the standards in this document.

9.1. Apple Developer and App Store Connect

- Third-party developers must use their own Apple account to access Apple Developer and App Store Connect
- When access is requested, the Mobile App Service will grant the third-party developer the **App Manager** role
 - **App Manager** is the highest role a third-party developer will be granted

9.2. Google Play Store

- The Mobile App Service will create a Service Account within Google Play for the third-party developer
- The following named App Permissions will be granted when access is requested:
 - "View App Information (read-only)"
 - "Edit and delete draft apps"
 - "Release to production, exclude devices, and use Play App Signing"
 - "Manage Store Presence"

Google Play processes are anticipated to change to a model more like that of the Apple Store. Suppliers of existing third-party apps will be notified of the changes to process. New suppliers should ensure they are familiar with current Google Play store roles.

10. Access Request Protocol

Access to University App Stores is by request only, and only for a limited time window agreed in advance that must be:

- UK business hours 9am - 5pm
- On a [working day for the University of Strathclyde](#)
- Out with the University's change freeze periods which generally align with the formal assessment periods at the University (confirmation of dates can be provided by the Mobile App Service on request)
- On a day other than Friday where the access is to perform a release, unless for an essential security update

The third-party developer's account will be granted the appropriate roles or permissions that will allow them to manage the App they are responsible for (as outlined above in [Section 10](#)).

To request access, a third-party must:

- Contact your University Business Partner to raise a ticket with the University's IT Helpdesk.
- Include as much detail as possible on what work will be performed during the access period and whether a release from the University App Stores is anticipated. Where a release is anticipated, a change request will be generated for the relevant Change Advisory Board and enough detail about the nature and content of the release must be provided or approval for the release will not be granted.
- Submit the request in time to allow your University Business Partner to give at least five working days' notice when submitting their request (these must be [University working days](#)).
- Indicate the desired start time of your access.

If the access request is successful, you will be granted access to the specified University App Stores for one working day (09:00 – 17:00, UK business hours).

Any requests for access periods longer than four hours must be negotiated with, and approved by, the Mobile App Service and your access request submitted at least five working days in advance.

11. Release protocols

It is required that new releases for third-party apps are delivered through both the Apple App Store and the Google Play Store concurrently. It is not acceptable to issue a release to one store and not the other unless to address a store-specific issue only.

The only way to achieve this is to trigger the releases manually after both have been fully approved by the app stores. This can be managed in one of two ways:

1. The third-party supplier requests that the releases are manually triggered by a member of the Mobile App Service after the app store approval processes have completed. This must be clearly stated in the initial access request and will be subject to agreement by the Mobile App Service.
2. The third-party supplier must request an additional period of access in order to manually perform the releases. This must be clearly stated in the initial access request and will be subject to agreement by the Mobile App Service.

12. Testing

It is expected that third-party suppliers will thoroughly test their app prior to release. This testing should encompass, but is not limited to, cyber security provisions, data protection assurance, digital accessibility compliance, push notification functionality, and all functional and user acceptance testing. The Mobile App Service should be provided with access to test versions (Test Flight, Beta, etc), in case they are required.