

附件 9 模型共享使用管理計劃

子計畫名稱： 上傳範例 (下稱本計畫)

子計畫主持人： 王大同

資料庫或 AI 模型名稱/編號： 飯粒資料庫

(備註：一個資料集或 AI 模型請填寫一份附件表格)

填表人： 王大同

填表日期： 2099 年 2 月 29 日

##底下請自由發揮一下

備註：下表一項資料集請填寫一份，表格不敷使用請自行增列。

一、AI 模型來源盤點程序

計畫團隊應建立 AI 模型來源盤點程序，納入資料與模型治理作業規範中，主要盤點項目包括：授權型態、授權條款類型與版本、授權範圍與條件

事項內容						回應
關於「授權型態」，計畫團隊所引用的程式庫是採傳統商業授權或自由/開源授權？ ※備註：即使所引用的程式庫屬於自由/開源軟體(Free/Open Source Software)，也不等同於可完全無償且無條件使用。						☐ 傳統商業授權 ☒ 自由 / 開源授權，授權條款類型與版本為： *請繼續勾選 *若同個資料集採用不同套件，可複選 ☐ MIT ☐ GPL（最嚴謹） ☐ LGPL ☐ APACHE ☐ Only new BSD license ☒ Simplified BSD license（最寬鬆） ☐ 其他：_____
條款	GPL	LGPL	BSD	APACHE	MIT	
公開原始碼	✓	✓				
以同樣方式授權	✓					
標註修改的部分	✓	✓		✓		
必須包含 Copyright	✓	✓	✓	✓	✓	
必須包含 License	✓	✓		✓	✓	

<pre> graph TD Q1[衍生品可否不開源並且商業使用] -- NO --> Q2[是否需要相同License] Q1 -- Yes --> Q3[衍生作品是否需要放置版權說明] Q2 -- NO --> LGPL Q2 -- Yes --> GPL Q3 -- NO --> Q4[可否用原作者進行推廣、推薦或是鳴謝] Q3 -- Yes --> Apache Q4 -- NO --> BSD1[Only new BSD license] Q4 -- Yes --> BSD2[Simplified BSD license] </pre> 針對修正處須提供說明文字檔	
※前一題若選擇自由 / 開源授權者，才須回答此題 承上，關於「授權範圍與條件」，計畫團隊所引用的程式庫之授權條款對於利用該程式庫所「衍生」之作品，有無任何限制？就該「衍生」之作品，第三方使用者是否須透過與原程式庫（原作品）同等條件散布或再授權？ ※備註：所謂「衍生」之作品即為「衍生著作」，係指就原著作改作之創作，以獨立的著作保護之，著作權法第 6 條訂有明文。	x 無任何限制（Simplified BSD license 屬此） ☐ 有限制 *請繼續勾選 *以下限制由寬鬆到嚴格依序排列 *若同個資料集採用不同套件，應選取「最嚴格」的授權敘述 ☐ 衍生之作品可不共享且可營利，並且不可用原作者進行推廣或推薦（Only new BSD license 屬此） ☐ 衍生之作品可不共享且可營利，並且衍生作品需要放置版權說明（Apache、MIT 屬此） ☐ 衍生之作品必須共享且不可營利，並且不須透過同等條件散布或再授權（LGPL 屬此） ☐ 衍生之作品必須共享且不可營利，並且須透過同等條件散布或再授權（GPL 屬此）

關於「授權範圍與條件」，計畫團隊所引用的程式庫，除了授權使用之外，是否能被複製、修改、合併、散布、再授權及 / 或販售予他人？	☐ 是 ☐ 否
關於「授權範圍與條件」，計畫團隊所引用的程式庫之授權條款對於利用該程式庫所「衍生」之作品，有無任何限制？就該「衍生」之作品，第三方使用者是否須透過與原程式庫（原作品）同等條件散布或再授權？ ※備註：所謂「衍生」之作品即為「衍生著作」，係指就原著作改作之創作，以獨立的著作保護之，著作權法第 6 條訂有明文。	☐ 無任何限制 ☐ 有限制，不過「衍生」之作品不須透過同等條件散布或再授權 ☐ 有限制，而且「衍生」之作品須透過同等條件散布或再授權

二、可信賴 AI 檢核程序

事項內容	是否同意
計畫團隊應建立可信賴 AI 檢核程序，將可信賴 AI 檢核要求納入資料與模型治理作業規範中，並確保計畫團隊之落實。	☒ 同意 ☐ 不同意
計畫團隊應參考科技部 2019 年提出的「人工智慧科研發展指引」(AI Technology R&D Guidelines)，建立適切之可信賴 AI 檢核表，並依據檢核結果，思考或規劃當前或未來可行的改善方法。 ※備註：「人工智慧科研發展指引」(AI Technology R&D Guidelines)中由三大價值衍生構築出之 八大指引，包含「共榮共利、公平性與非歧視性、自主權與控制權、安全性、個人隱私與數據治理、透明性與可追溯性、可解釋性、問責與溝通」，詳參： https://www.most.gov.tw/most/attachments/53491881-cb0d-443f-9169-1f434f7d33c7	☒ 同意 ☐ 不同意
承上，計畫團隊應符合科技部 2019 年提出的「人工智慧科研發展指引」(AI Technology R&D Guidelines)中之共榮共利指引。	☒ 同意 ☐ 不同意

承上，計畫團隊應符合科技部 2019 年提出的「人工智慧科研發展指引」(AI Technology R&D Guidelines)中之公平性與非歧視性指引。	☒ 同意 ☐ 不同意
承上，計畫團隊應符合科技部 2019 年提出的「人工智慧科研發展指引」(AI Technology R&D Guidelines)中之自主權與控制權指引。	☒ 同意 ☐ 不同意
承上，計畫團隊應符合科技部 2019 年提出的「人工智慧科研發展指引」(AI Technology R&D Guidelines)中之安全性指引。	☒ 同意 ☐ 不同意
承上，計畫團隊應符合科技部 2019 年提出的「人工智慧科研發展指引」(AI Technology R&D Guidelines)中之個人隱私與數據治理指引。	☒ 同意 ☐ 不同意
承上，計畫團隊應符合科技部 2019 年提出的「人工智慧科研發展指引」(AI Technology R&D Guidelines)中之透明性與可追溯性指引。	☒ 同意 ☐ 不同意
承上，計畫團隊應符合科技部 2019 年提出的「人工智慧科研發展指引」(AI Technology R&D Guidelines)中之可解釋性指引。	☒ 同意 ☐ 不同意
承上，計畫團隊應符合科技部 2019 年提出的「人工智慧科研發展指引」(AI Technology R&D Guidelines)中之問責與溝通指引。	☒ 同意 ☐ 不同意

三、AI 模型提供使用（共享）之規劃

(一) AI 模型提供使用條件

事項內容	回應
是否需對 AI 模型的使用對象加以限制？ ※備註：只需要針對「填表當下目前已知資訊」去填寫	☐ 是，AI 模型使用對象限於： _____ ☐ 否 (包括目前仍不清楚是否需對 AI 模型的使用對象加以限制)
若預定上架的模型是改作他人模型，依據原模型（改作前的模型）的授權情況，預定上架的 AI 模型需以何種方式再授權他人使用？	☐ 傳統商業授權 ☐ 自由/開源授權 ※自由/開源授權，包含：MIT 授權條款(MIT License)、GNU 通用公眾授權條款(GNU General Public License, GPL)等。
若預定上架的 AI 模型，是由模型提供者完全原創，依據模型共享預期的目標，預定上架的 AI 模型需以何種方式再授權他人使用？	☐ 傳統商業授權 ☐ 自由/開源授權 ※自由/開源授權，包含：MIT 授權條款(MIT License)、GNU 通用公眾授權條款(GNU General Public License, GPL)等。

(二) AI 模型提供使用方式

事項內容	回應
依 AI 模型來源法律關係與可信賴 AI 檢核結果，AI 模型提供使用方式為何？ (例如：使用者可否取得程式原始碼等)	使用方式： _____ _____
如何確保 AI 模型取得是安全的？ 為避免 AI 模型發生資安問題，請說明所採用的手段。	手段 / 方案： _____ _____

承上，發生資安事故時，計畫團隊應如何處理？	處理方式： _____ _____
-----------------------	-------------------------

(三) AI 模型使用回饋

事項內容	回應
計畫團隊共享 AI 模型所欲達成的願景或目標為何？	願景或目標： _____ _____
承上，以此願景或目標為基礎，預期 AI 模型使用者要如何提供回饋？（可複選）	☐ AI 模型使用成果預設授權予模型提供者使用 ☐ 使用者回饋有助於提升 AI 模型準確度的訓練或測試資料 ☐ 使用者回饋 AI 模型使用經驗 ☐ 其他回饋方式： _____ _____ _____

(四) AI 模型使用情況追蹤、模型提供服務之改善

事項內容	回應
計畫團隊採取何種機制以瞭解 AI 模型使用的情況？	所採用之機制： _____
AI 模型使用的情況，是否符合計畫以外使用者的需求或期待？	☐ 是 ☐ 否 ☐ 無從得知，因計畫外的使用者

	沒有回覆
AI 模型使用過程中， 計劃以外的使用者 是否有發生問題或障礙？	☐ 是，發生的問題或障礙： ☐ 否 ☐ 無從得知，因計畫外的使用者沒有回覆
承上，計畫團隊在瞭解 AI 模型使用情況後，採取 何種機制 進行相應的改善或優化？	☐ 技術團隊提供給 計畫外的使用者 email 或其他聯絡管道 ☐ 其他機制：
AI 模型共享對 計劃以外的使用者 所產生之效益為何？ ※若無從得知，請據實填寫	☐ 效益： ☐ 無從得知，因計畫外的使用者沒有回覆

四、AI 模型上架

是否有預計施行 AI 模型上架？ ☐ 是，**請繼續填寫**以下表格 ☐ 否，**不需填寫**以下表格

事項內容	回應
計畫團隊將 AI 模型上架至共享平台供他人使用前，應先建立 AI 模型簡介或說明。	☐ 同意 ☐ 不同意
計畫團隊若欲將 AI 模型放到「非自建」之共享平台供他人使用，AI 模型上架前，計畫團隊應與「共享平台服務提供者」透過委託書、契約等文件，預先議定彼此的權利義務。應注意議定事項包括： (1) 預定上架及存放於平台的 AI 模型及期限（委託範圍與期限）。 (2) 委託範圍內 AI 模型品質之維護方式。 (3) 平台對於 AI 模型之安全維護與保密要求。	☐ 同意 ☐ 不同意

- | | |
|---|--|
| <p>(4) 發生 AI 模型被竊取、竄改、毀損、滅失或洩漏等事故時，平台之通報義務。</p> <p>(5) 要求平台對其使用者（計劃以外的使用者）規範使用 AI 模型的條件、形式與方法。</p> <p>(6) 違約責任。</p> <p>(7) 紛爭處理。</p> | |
|---|--|