新竹市政府
公開文件敏感資料遮蔽風險及防範指引

1 公開文件敏感資料未有效遮蔽風險

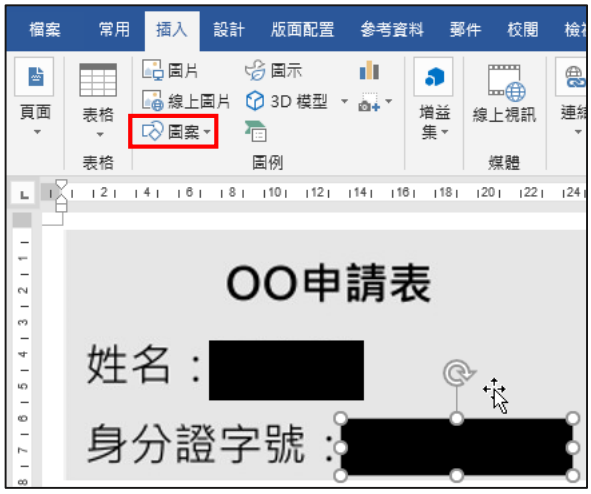
◆ 資料外洩風險

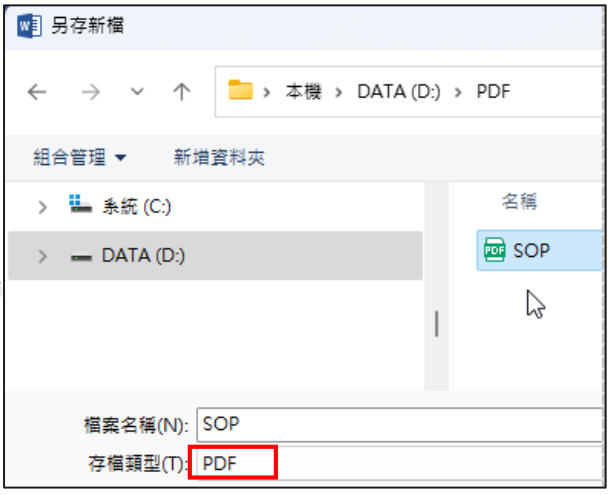
依國家資通安全研究院之「政府機關資安威脅與防護重點」中提出以下：

- 機關為方便民眾操作網站服務，**提供說明文件檢附實際申請書或操作畫面範例**。
- 部分文件圖片之敏感資料遮蔽處理，僅於圖片加上黑色方塊或其他圖層，底層之完整圖片資料仍保留於文件中，有心人士可透過Adobe Reader複製底層圖片並存放於其他文件，進而檢視被遮蔽內容，使敏感資料存在外洩之風險。

資料外洩操作示例

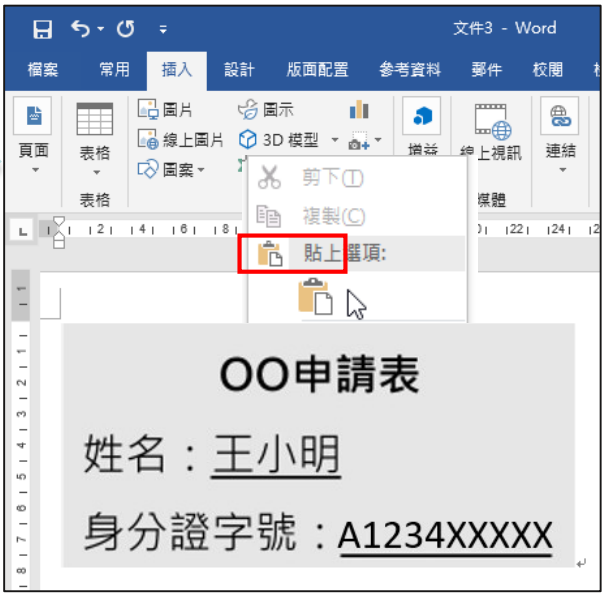
1. 在Word中使用 黑色方塊 遮蔽敏感資料後，將文件轉存為PDF文件。





2. 打開PDF文件並於該圖片上點右鍵選擇複製影像。

3. 將複製的圖片貼到word文件，會看到原本在word檔用黑色方塊遮蔽之敏感資料，造成敏感資料外洩。



⚠ 使用黑色方塊或圖層遮蔽資料，**表面看似遮蔽，但實際上底層資料未被完全移除或加密**，使得有心人士可透過複製底層圖片，繞過遮蔽查看敏感資料，增加資料外洩風險，進而對機關和民眾造成資安危害。

新竹市政府
公開文件敏感資料遮蔽風險及防範指引

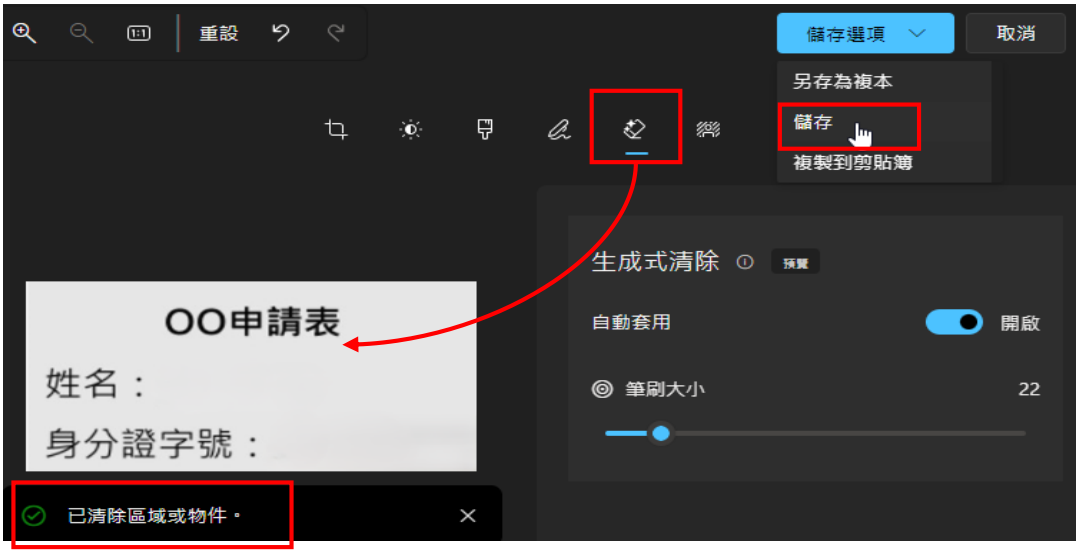
2 敏感資料遮蔽處理方法

◆ 遮蔽處理方法

- 方法一：直接在文件(例如word文件)上將部分敏感資料「替換為無意義的符號」，例如「王小明」改成「王OO」，身分證字號改成「A*********」，確保敏感資訊不被洩漏。
- 方法二：使用圖片處理工具轉換為單一圖層圖片，如windows相片、小畫家、修圖軟體或截圖軟體另行編輯，將敏感資料遮蔽後重新儲存為圖片，再貼入文件中(附圖1)。
- 方法三：使用PDF「標記密文」工具(pdf專業版才有此功能)，框住要從PDF中移除的文字或影像 (附圖2)，進行永久性清除 。

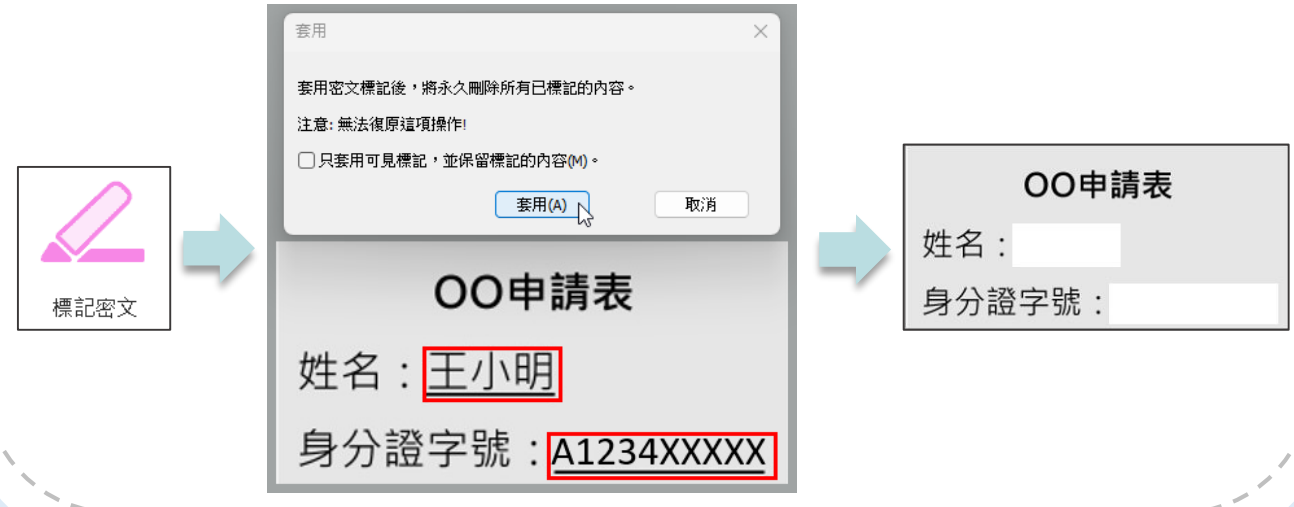
附圖1

在windows相片中選擇「編輯→清除」，將敏感資料清除後，另儲存為圖片。



附圖2

在PDF選擇「標記密文」→框住要從 PDF 中永久移除的文字或影像後→選「套用密文」存檔，敏感資料即清除。



新竹市政府
公開文件敏感資料遮蔽風險及防範指引

3 敏感資料遮蔽處理原則

◆ 遮蔽處理的基本原則

- 需有效遮蔽敏感資料，防止資料被還原或洩漏。
- 識別敏感資料範圍：如個人資料、財務資料、機密資料等。

① 僅提供少數相關業務承辦人員及其主管，或被授權之單位及人員使用。

② 發生資通安全事件可能造成未經授權之資訊揭露，對機關之營運、資產或信譽等方面將產生非常嚴重或災難性之影響。

◆檢查與驗證防護：

- 確保遮蔽後的資料無法被還原，避免僅是簡單的視覺遮擋，防止心懷不軌者透過工具輕易還原資料。
- 在網站公開資訊或上傳附件前，應確實全面檢視(如文件檢查清單)，如具有敏感資料應**確保敏感資料已移除或確實遮蔽處理完成**。

文件檢查清單：

- ☐ **文件中是否包含任何敏感資料？**
- ☐ **所有圖片中的敏感資料是否已進行有效遮蔽(複製底層圖片測試是否仍能看見敏感資料)？**
- ☐ **所有文本中的敏感資料是否已經替換為無意義符號或完全刪除？**
- ☐ **必要時請兩名以上的同仁進行複查，確認無遺漏?**