社会福祉法人松花苑 特定個人情報等取扱規程

（目的）

第１条　この規程は、行政手続における特定の個人を識別するための番号の利用等に関する法律（以下「番号法」という）及び特定個人情報保護委員会が定める「特定個人情報の適正な取扱いに関するガイドライン（事業者編）」に基づき、社会福祉法人　松花苑（以下「法人」という）における個人番号及び特定個人情報（以下「特定個人情報等」という）の取扱いについて定めたものである。

（定義）

第２条　この規程における各用語の定義は以下のとおりとする。

（１）個人情報

生存する個人に関する情報であって、当該情報に含まれる氏名、生年月日その他の記述等により特定の個人を識別することができるもの（他の情報と容易に照合することができ、それにより特定の個人を識別することができることとなるものを含む。）をいう。

（２）個人番号

住民票コードを変換して得られる番号であって、当該住民票コードが記載された住民票に係る者を識別するために指定されるものをいう。

（３）特定個人情報

個人番号（個人番号に対応し、当該個人番号に代わって用いられる番号、記号その他の符号であって、住民票コード以外のものを含む。番号法第７条第１項及び第２項、第８条並びに第 67 条並びに附則第３条第１項から第３項まで及び第５項を除く。）をその内容に含む個人情報をいう。

（４）個人番号利用事務

行政機関、地方公共団体、独立行政法人等その他の行政事務を処理する者が番号法第９条第１項又は第２項の規定によりその保有する特定個人情報ファイルにおいて個人情報を効率的に検索し、及び管理するために必要な限度で個人番号を利用して処理する事務をいう。

（５）個人番号関係事務

番号法第９条第３項の規定により個人番号利用事務に関して行われる他人の個人番号を必要な限度で利用して行う事務をいう。

（６）個人番号関係事務実施者

個人番号関係事務を処理する者及び個人番号関係事務の全部又は一部の委託を受けた者をいう。

（7）通知カード

平成 27 年 10 月以降、市区町村から住民票の住所に送付され、本人の氏名、住所、生年月日、性別、個人番号が記載される紙製のカードをいう。

（8）個人番号カード

氏名、住所、生年月日、性別、個人番号その他政令で定める事項が記載され、本人の写真が表示され、かつ、これらの事項その他総務省令で定める事項（以下「カード記録事項」という。）が電磁的方法（電子的方法、磁気的方法その他の人の知覚によって認識することができない方法をいう。）により記録されたプラスチック製の IC チップ付カードをいう。

（取扱い業務の範囲）

第３条　法人が取扱う特定個人情報等は、原則として以下のとおりとする。

（1）職員の所得税法等の税務関連の届け出事務

（2）社会保険及び労働保険関連の届け出事務

（3）報酬・料金等の支払調書作成事務

（4）配当、余剰金の分配に関する支払調書作成事務

（5）不動産の使用料等の支払調書作成事務

（6）不動産等の譲受けの対価の支払調書作成事務

（7）上記に付随する行政機関への届け出事務

（組織体制）

第４条　特定個人情報等の取扱いについての組織体制は、以下のとおりとする。なお、担当者及び担当職が不在の場合はその代行者が担当者となる。

個人情報等の取扱いに関する最高責任者（全体統括）	理事長
運用責任者	施設長
安全管理対策責任者	施設長が指名した職員
事務取扱担当者	事務職員

（守秘義務）

第５条　特定個人情報等を取り扱うすべての者は、徹底した守秘義務の中で業務を遂行しなければならない。

（法令等の遵守）

第６条　法人は、番号法及び特定個人情報保護委員会が定めた「特定個人情報の適正な取扱いに関するガイドライン（事業者編）」を遵守して運用をする。

（責任者の役割）

第７条　各責任者の役割は、以下のとおりとする。

特定個人情報等の取扱いに関する 最高責任者（全体統括）	運用責任者及び安全管理対策責任者を監督し、特定個人情報等の取扱い等についてのすべての最終的な責任を負う
運用責任者	職員への教育や啓蒙、更には安定的な継続運用のために企画を実施し、管理等を行う役割を担う
安全管理対策責任者	システム及び物理的な対策を講じて情報が漏えいすることがないような体制を整える役割を担う

（情報漏えい対応策）

第８条　各責任者及び事務取扱担当者は、情報漏えい発生時またはその可能性が疑われる場合には、速やかに所属長及び運用責任者に報告をするとともに漏えいの拡大を阻止するように対策を講じなければならない。

２．各責任者は、情報漏えい発生時またはその可能性が疑われる場合には、事後に速やかにその原因を究明して最高責任者に報告をしなければならない。

３．最高責任者及び運用責任者は、情報漏えい時には関係官庁への連絡を行なうとともに速やかに原因や再発防止策を公表しなければならない。

４．運用責任者は、情報漏えい時には、影響を受ける可能性がある本人への連絡を速やかに行わなければならない。

５．法人は必要に応じて、外部の機関やコンサルティング法人等より監査を受ける等の対策を講じることがある。

（特定個人情報ファイル作成の制限）

第９条　個人番号を取扱う者は、法令に基づき行う事務手続きに限って、特定個人情報に関するファイルを作成することができ、これらの場合を除いて特定個人情報ファイルを作成してはならない。

（個人番号の提供の要求）

第 10 条　法人は、個人番号関係事務を行うために、本人または他の個人番号関係事務実施者若

しくは個人番号事務実施者に対して、個人番号の提供を求めることができる。

（第三者提供の停止）

第11条　特定個人情報が違法に第三者に提供されていることを知った本人からその提供の停止を求められた場合であって、その求めに理由があることが判明したときには、第三者への提供を停止しなければならない。

（取得）

第12条　事務取扱担当者は、特定個人情報等の提供を受けるにあたっては、その写しを紙によって受領しなければならない。ただし、オンライン環境によってその受領の必要性がない場合には、その限りではない。

２．事務取扱担当者は、通知カード及び個人番号カードの原本を受領してはならない。（ただし、コピー後、すぐに返還する場合はこの限りではない）

３．事務取扱担当者は、通知カード及び個人番号カードを撮影してはならない。ただし、安全管理対策責任者が特別に認めた機器があれば、その機器によってのみ撮影をすることができる。

４．職員以外の対象者から特定個人情報等の提供を受ける場合には、法人所定の用紙にて届出てもらう。

５．事務取扱担当者は、提出された特定個人情報等の写しを速やかに情報システムに入力若しくは、ファイルし厳重に保管しなければならない。

６．事務取扱担当者は、情報システムに入力をした特定個人情報等の確認のために印刷をしてはならない。

（利用）

第13条　取扱い事務担当者は、情報システムを利用して第３条に定める事項について申告書や申請書等を作成することができる。

２．前項の申告書や申請書等は、行政機関等への提出分につき印刷をすることができる。

３．情報システムの利用にあたっては、安全管理対策責任者の指示による方法でしか利用することができない。

４．事務取扱担当者は、行政機関への提出及び調査等の場合に限り、安全管理対策責任者の許可を得て施設外（立入り禁止区域外の場所の移動も含む）に持出すことができる。この場合、紙媒体の資料のみ許可し、デジタル媒体による持出しはできない。

５．前項において、オンライン上で申請等を行う場合には、安全管理対策責任者が定めた手順によって行なうことができる。

６．安全管理対策責任者は、行政機関等への申請その他の利用状況につき、事務取扱担当者のパソコン等の機器をモニタリングすることができる。事務取扱担当者は、モニタリングを拒

否することはできない。

7．各事業所への特定個人情報等の連絡にあたっては、電子メールの場合には法人指定のアドレスを使用すると同時に、添付ファイルがある場合には必ずパスワードをつけて送信しなければならない。

8．特定個人情報等の利用にあたっては、如何なる場合であってもＦＡＸによる送受信は行ってはならない。

9．特定個人情報等が記載された書類をその対象者に渡す場合には、密封式の封筒を用いるものとし、職員の場合は所属長を通じて手渡し、職員以外の場合は簡易書留によって郵送することを原則とする。

（保存）

第 14 条　特定個人情報等は、それが記載された書類等に係る関係法令に定める期間保存をする。

2．紙媒体の特定個人情報等が記載された資料は、鍵付きのキャビネットに保管する等の方法により管理をする。なお、この鍵は、運用責任者または安全管理対策責任者のみが所持することができ、原則として毎日始業時に開錠し、終業時に施錠をする。

3．特定個人情報等は、その情報がデジタル情報による場合には、情報システム等の安全管理対策責任者が定めたソフトウェア等によってのみ保存することができ、事務取扱担当者が扱うパソコンやネットワーク上の共有フォルダ等に保存してはならない。

（提供）

第 15 条　特定個人情報等は、関係法令により必要な場合においてのみ関係行政官庁へ提供することができる。

2．前項の提供にあたっては、簡易書留の利用等の方法により、厳重な管理方法によって提供を行わなければならない。

3．出向者または転籍者については、改めて通知カードまたは個人番号カードを提示してもらうことにより個人番号を法人に提供してもらわなければならない。

（削除・廃棄）

第 16 条．特定個人情報等は、関係法令により定められた保存期間を超えた場合に削除・廃棄を行うものとする。

2．特定個人情報等の紙媒体の廃棄にあたっては、完全焼却・溶解処分・マスキング（塗りつぶす）・シュレッダーにて裁断など、安全確実な方法で行わなければならない。

3．デジタル情報によるデータの削除については、安全管理対策責任者が指示した者によって処理をするものとし、事務取扱担当者が自己の判断によって削除をしてはならない。

4．特定個人情報等を取扱ったパソコンを処分する場合は、法人が指定する業者により粉砕など復旧不可能な処理を施さなければならない。この場合、事後に証明書を発行してもらわな

ければならない。

（収集の制限）

第17条　法人は、第３条に定める事務の範囲を超えて特定個人情報等を収集してはならない。

（本人確認）

第18条　法人は、番号法第１６条の定めにより個人番号所有者の番号確認及び身元確認を行うものとする。この場合、代理人により身元確認等を行う場合には、代理者からの委任状を提出してもらわなければならない。

（組織的安全管理措置）

第19条　法人は、組織的安全管理措置を講じるために以下を実施する。

（１）情報漏えい等の事案発生時には、昼夜を問わず運用責任者及び安全管理対策責任者の携帯電話へ連絡することができるようにそれぞれの責任者の携帯電話番号及びメールアドレスを関係部署へ公開する。

（２）不定期による情報漏えい事故対策訓練を実施する。

（３）情報システムで特定個人情報ファイルを取り扱う際は、情報システムのアクセスログを記録する。

（人的安全管理措置）

第20条　法人は、人的安全管理措置を講じるために以下を実施する。

（１）特定個人情報等の取扱いに関する留意事項等について、関係部署職員に対して定期的な研修を実施する。

（２）特定個人情報等についての秘密保持については、就業規則においても明確化し、そのルールを周知する。

（物理的安全管理措置）

第21条　法人は、物理的安全管理措置を講じるために以下を実施する。

（１）安全管理対策責任者が定めた者以外は立入ることができないように立入り禁止区域を定める。

（２）特定個人情報等を取扱うパソコンは、セキュリティワイヤーにより固定をするなど、適切な方法で盗難防止対策を講じる。

（技術的安全管理措置）

第22条　法人は、技術的安全管理措置を講じるために以下を実施する。

（１）システムへのアクセスは、アクセスすることができる担当者を限定し、そのアクセス状

況を記録する。

（2）情報システムと外部ネットワークとの接続箇所にファイアウォールを設置し、不正アクセスを遮断する。

（3）情報システムへのログインにあたってのパスワードは、定期的に変更・更新をする。

（特定個人情報等の取扱い委託）

第23条　法人は特定個人情報等の取扱いについて、外部業者等に委託をすることができる。この場合、理事会による承認を得なければならない。

2．前項における委託先は、組織的・人的・物理的・技術的な安全管理措置が客観的に講じられているところでなければ委託をしてはならない。

（特定個人情報等の取扱い再委託）

第24条　特定個人情報等の取扱いの再委託は、理事会の承認により再委託することができる。

（事務取扱い担当者への監督）

第25条　運用責任者及び安全管理対策責任者は、事務取扱担当者に対しての管理及び監督をするものとし、運用方法について情報漏えいの可能性がある場合には、是正に向けて指図をしなければならない。

2．前項における監督にあたり、安全管理対策責任者は必要に応じて是正の指図をすることができる。

（苦情や相談等の対応）

第26条　特定個人情報等の取扱いについての苦情や相談等の対応は、運用責任者が担当して対応する。

（違反時の対応）

第27条　この規程に違反する行為がみられた場合には、就業規則に基づき懲戒処分に科すことがある。

（規程の改定）

第28条　法人は、必要に応じて本規程を改定する。

附　　則

この規則は平成２８年１月１日から施行する。