

# 特定非営利活動法人グッドネーバーズ・ジャパン

## 情報管理規程

### 第一編 秘扱文書情報管理

#### 第一章 総括

##### 第1条（総則）

この規程の第一編は、特定非営利活動法人グッドネーバーズ・ジャパン（以下「団体」という）の保有する秘扱文書・情報の管理について定める。本規程は団体において雇用する全ての職員等に対して適用する。

##### 第2条（定義）

この規程において「秘扱文書・情報」とは、団体の経営上きわめて重要で、その内容が他に漏れると運営に重大な支障が生じる情報が記載または記録されている文書、または媒体をいう。

##### 第3条（区分）

秘扱文書・情報は、その機密度に応じて、次の2つに区分する。

###### （1）極秘情報

団体内の関係者以外には知られてはならない以下の情報。

- ① 経営戦略・予算・分析データ等、団体の運営の根幹にかかわる重要情報で、団体のホームページに公開している情報以外のもの。
- ② インターネットバンキングにかかわる情報
- ③ 人事等個人の機密にかかわる情報。
- ④ その他、上記に準ずる機密事項に関する情報。

###### （2）外秘情報

団体外には知られてはならない情報。

- ① 各種インターネットサイトへのログインIDとパスワード
- ② 各事業に関わる非公開情報
- ③ その他、団体外に知られては不都合な情報

#### 第4条（区分の決定）

文書または情報を機密扱いとすること、および秘扱文書・情報の区分の決定は、その文書または情報を作成した部門長が行う。

#### 第5条（区分の表記）

部門長は、作成した文書または情報について機密扱いとすることを決定したときは、その文書の表紙または1ページ目に区分（極秘情報・外秘情報）を明記して管理しなければならない。

#### 第6条（スタッフの義務）

- （1）スタッフは、この規程を誠実に遵守して秘扱文書・情報を管理しなければならない。
- （2）スタッフは、インターン・ボランティア等に秘扱文書・情報を扱わせる場合、常に監視下に置き、本規程の意図するところを良く理解させ、情報管理を徹底させる。
- （3）支援者情報の管理については、常識と良識をもって対応し、判断に迷うときは上司の指示を求めなければならない。

## 第二章 管理体制・管理方法

#### 第7条（管理責任者）

##### （1）情報管理責任者

本規程の維持・管理を目的として、事務局長を「情報管理責任者」とし、部門長を「情報管理一次責任者」とする。情報管理一次責任者は情報管理責任者の指示に従い、常に報告を怠らないようにすること。

##### （2）情報管理一次責任者

部門長は、情報管理一次責任者として文書・電子データの廃棄状況、管理状況、施錠管理等の状況、プリンター周り等の共用部分の整備状況に留意し、常に職場環境の維持整備にあたる事とする。

#### 第8条（保管場所および保管期間）

秘扱文書・情報（含む複写）は、鍵またはセキュリティ（含むパスワードの設定）のかかるフォルダーやキャビネット等に保管しておかななければならない。秘扱文書・情報が不要になった時から5年を経過したものは、手続きに従い廃棄処分とする。

#### 第9条（点検の義務）

情報管理一次責任者は、秘扱文書・情報（含む複写）が確実に保管または管理されているかどうかを、定期的に点検し、職場環境の整理・整頓状況と共に、情報管理責任者に報告し

なければならない。

#### 第10条（引き継ぎの義務）

情報管理一次責任者は、人事異動または退職の際には、情報管理責任者が指定した後任者との間において、秘扱文書・情報の引き継ぎを確実に行わなければならない。

#### 第11条（複写の手続き）

（1）スタッフは、業務上の必要によって秘扱文書または情報を複写し外部に持ち出す時は、あらかじめ情報管理一次責任者に次の事項を申し出て、その許可を得なければならない。

- ① 所属、氏名
- ② 秘扱文書または情報の名称
- ③ 持ち出し先及び目的
- ④ 持ち出す日時(期間)

（2）秘扱文書または情報を複写したときは、その取扱いに十分注意しなければならない。

## 第二編 支援者情報管理

### 第一章 総括

#### 第12条（総則）

（1）この規程の第二編は、「支援者情報」の管理について定める。

（2）支援者情報管理に関して、この規程に定めのない事項については、個人情報保護法の定めるところによる。

#### 第13条（支援者情報の定義）

この規程において「支援者情報」とは以下に定義した情報とし、紙、電子データなど媒体の種類は問わない。

##### ①個人情報

支援者の氏名、住所、電話番号、生年月日、寄付状況等、特定の個人を識別することのできる情報をいう。

##### ②業務上知り得た情報

業務上で知り得た商品知識、商流、物流、取引実態、契約、報告書および支援者からの預かり情報などで、特定の事案または企業を識別することのできる情報（公表されているものを除く）をいう。

#### 第14条（スタッフの義務）

（1）スタッフは、この規程を誠実に遵守して支援者情報を管理しなければならない。

（2）スタッフは、インターン・ボランティア等に支援者情報を扱わせる場合、常に監視下に置き、本規程の意図するところを良く理解させ、情報管理を徹底させる。

（3）支援者情報の管理については、常識と良識をもって対応し、判断に迷うときは上司の指示を求めなければならない。

### 第二章 利用制限および取得

#### 第15条（情報利用の制限）

（1）スタッフは、次の場合を除いて支援者情報を第三者に提供してはならない。

① 予め、本人あるいは当事者の同意書がある場合

② 団体の業務達成に必要な範囲で、業務委託先に情報を提供する場合

③ 情報を特定の者との間で相互に利用する場合で、予めその利用目的・提供先等について本人に通知されているか、または公表が行われている場合

（2）前項の規定は、法令に基づく場合については適用しない。

#### 第16条（適正な取得）

（1）団体は、適法かつ適正な方法で支援者情報を取得する。

（2）第三者から情報を取得する場合は、第三者が適法かつ適正な方法で取得した情報であることを確認のうえ取得する。

#### 第17条（取得しない支援者情報）

団体は、次に掲げる支援者情報は取得しないものとする。

① 思想、信条および宗教に関する事項

② 人種、民族、社会的身分、門地、本籍地（所在都道府県に関する情報は除く）、心身の障害、犯罪歴、その他社会的差別の原因となる事項

③ その他、取得することがふさわしくない事項

#### 第18条（内容の正確性の確保）

団体は、利用目的の達成に必要な範囲内において、支援者情報を正確かつ最新の内容に保つよう努めるものとする。

### 第三章 管理体制・管理方法

#### 第 19 条（管理責任者）

情報管理責任者及び情報管理一次責任者の定義は第 6 条と同じ。

#### 第 20 条（保管場所および保管期間）

（1）情報管理一次責任者は、支援者情報を鍵またはセキュリティ（含むパスワードの設定）のかかる保管場所に保管しておかなければならない。

（2）支援者情報の複写を保有している者も、同様の取り扱いをしなければならない。

（3）支援者情報は、不要になった時から 5 年を経過したものは、手続きに従い廃棄処分とする。

#### 第 21 条（点検の義務）

情報管理一次責任者は、支援者情報が確実に保管または管理されているかどうかを、定期的に点検し、職場環境の整理・整頓状況と共に、情報管理責任者に報告する。

#### 第 22 条（支援者情報の禁止事項）

スタッフは、いかなる事由があれ、支援者情報に関し、次に掲げることをしてはならない。

- ① 不正にアクセスすること
- ② 外部の者に漏えいすること
- ③ 業務以外の目的で使用すること
- ④ 不正に改ざんすること
- ⑤ その他、不正に行うこと

#### 第 23 条（複写などの手続き）

（1）スタッフは、支援者情報をコピーまたは撮影するときは、次の事項をあらかじめ情報管理一次責任者に申し出て、その許可を得なければならない。

- ① 利用目的
- ② コピーまたは撮影する支援者の範囲
- ③ コピーまたは撮影する支援者情報の範囲
- ④ コピーまたは撮影する日時
- ⑤ コピーまたは撮影する支援者情報の取扱い

（2）支援者情報をコピーまたは撮影したときは、その管理に十分注意しなければならない。

#### 第 24 条（社外への持ち出し禁止）

（1）スタッフは、支援者情報が記録されている媒体を社外に持ち出ししてはならない。

(2) 前項の規定は、次の各号をあらかじめ情報管理一次責任者に申し出て、その許可を得た場合はその限りでない。

- ①情報を持ち出す支援者の範囲
- ②持出す支援者情報の範囲
- ③持出し先及び目的
- ④持出す日時(期間)

(3) 支援者情報を社外へ持ち出したときは、その管理に十分注意しなければならない。

#### 第25条 (支援者情報の訂正など)

団体は、支援者から支援者の情報の内容が事実でないという理由によって、その内容の訂正、追加または削除（以下、「訂正など」という）を求められた場合には、速やかに訂正などを行う。

#### 第26条 (利用禁止など)

団体は、支援者から支援者情報の利用禁止または消去（以下、「利用禁止など」という）を求められた場合であって、その求めに正当な理由が判明したときは、速やかにその支援者情報の利用禁止などを行う。ただし、利用禁止などを行うことが困難な場合であって、支援者の権利利益を保護するため必要な代替え措置をとるときは、この限りではない。

## 第三編 共通管理事項

### 第一章 総括

#### 第27条 (総則)

この規程の第三編は、「秘扱文書・情報」および「支援者情報」の共通管理事項について定める。

### 第二章 情報品質保全

#### 第28条 (正確性の確保)

スタッフは秘扱情報および支援者情報は次の各号に定める所に従いその正確性の確保に努める。

- (1) 秘扱情報および支援者情報を記録する際は、細心の注意を払い正確に記録する。
- (2) 業務の達成に必要な範囲内において、可能な限り正確かつ最新の内容に保つこと。

## 第 29 条 (安全対策)

(1) 情報管理責任者および情報管理一次責任者は、秘扱情報および支援者情報の漏洩、紛失、滅失、毀損、破壊及び不当なアクセス・使用・改ざん等を防止するため、別表に定める安全対策を講じること。

(2) 情報管理責任者は、支援者情報漏洩事故発生時の被害者である支援者からの損害賠償請求に備えて、団体を守るために適切な情報漏洩損害保険に加入しておくこと。

## 第三章 廃棄処分

### 第 30 条 (廃棄処分の手続き)

スタッフは、「秘扱文書・情報」、「支援者情報」またはその両方が記録されている媒体を廃棄するときは、あらかじめ次の事項を情報管理一次責任者に届け出、廃棄の許可を得なければならない。

- ①支援者情報の範囲
- ②廃棄する理由
- ③廃棄する日時
- ④廃棄する方法
- ⑤その他の必要項目

### 第 31 条 (廃棄処分の方法)

スタッフは、「秘扱文書・情報」、「支援者情報」またはその両方を廃棄するときは、次のいずれかの措置を講じなければならない。

- ①シュレッダーによる裁断
- ②焼却または溶解
- ③復元し得ない方法によるデータ抹消措置または記憶媒体の物理的な破壊

## 第四章 不正行為への対応

### 第 32 条 (管理責任者への通知義務——不正行為対応)

(1) スタッフは、他のスタッフがこの規程に違反する行為を行ったことを知ったときは、次の事項を、原則知り得た当日に情報管理一次責任者または情報管理責任者に通報しなければならない。

- ① 行った者の氏名、所属
- ② 行った行為の具体的な内容

③ その他、知り得た事項

(2) 通報は、文書、口頭、電話、ファクシミリ、郵便、電子メールなど、その方法は問わないが、迅速を旨とする。

(3) 通報は匿名で行うこともできる。

第 33 条 (事実関係の調査)

(1) 情報管理一次責任者または情報管理責任者は、スタッフから違反行為の通報があったときは、直ちに事実関係を調査しなければならない。

(2) 事実関係の調査に当たっては、通報者に対して迷惑がかからないよう、十分配慮しなければならない。

第 34 条 (適切な措置の実施)

情報管理責任者は、事実関係の調査の結果、違反行為の事実が確認されたときは、直ちに適切な措置を講じなければならない

## 第五章 情報漏洩への対応

第 35 条 (管理責任者への通知義務——情報漏洩対応)

(1) スタッフは、情報の漏洩(以下、「情報漏洩」)が発生、またはその可能性を知ったとき(以下、「事故日」という)は、原則当日に情報管理一次責任者または情報管理責任者に通報しなければならない。

(2) 通報の第一報は、迅速な連絡方法(口頭または電話)とする。

第 36 条 (関係者への通知)

(1) 情報管理第一次責任者は、情報の漏洩について関係者へ 3 暦日以内に通知すること。

(2) 通知は、情報管理責任者が内容を確認の上おこなうものとし、原則書面とする。

第 37 条 (事実関係の調査)

(1) 情報管理一次責任者または情報管理責任者は、スタッフから情報漏洩の通報があったときは、直ちに事実関係を調査しなければならない。

(2) 情報管理責任者は、事実関係の調査を代理人に委譲できる。

## 第六章 情報漏洩の調査

### 第 38 条 （事実関係の調査と回収）

（１）団体は、「秘扱文書・情報」または「支援者情報」が外部へ流出または漏洩（以下、「漏洩」という）した時、または漏洩したおそれのある時は、その情報について直ちに次の調査をする。

- ①支援者の氏名（「支援者情報」の場合）
- ②秘扱文書・情報または支援者情報の範囲
- ③漏洩した日時
- ④漏洩した経緯、原因

（２）団体は「秘扱文書・情報」または「支援者情報」が漏洩した場合には以下の通り対処する。

#### （イ）（回収）

漏洩した情報の回収に最善を尽くす。

#### （ロ）（被害届・紛失届の提出）

必要に応じ警察に被害届を提出する。また、スタッフが情報の記録されている媒体を本人の不注意で紛失したときは、紛失届を提出する。

#### （ハ）（捜査への協力）

情報の漏洩に関する警察の捜査に全面的に協力する。

#### （ニ）（漏洩先の特定）

情報の漏洩先の特定に努める。

#### （ホ）（監視）

漏洩した情報が不正に使用されていないかを、継続的に監視する。

#### （ヘ）（漏洩先への要求）

漏洩先が特定されたときは、漏洩先に対し、漏洩した情報の返還を請求するとともに、その情報を使用しないように要請する。

#### （ト）（警告）

漏洩先が返還請求に応じない場合は、情報の漏洩先に対し、その情報を使用しないよう警告する。また漏洩先がその情報を使用したときは、使用を中止するよう警告する。警告は、内容証明郵便の送付により行う。

#### （チ）（差し止め請求）

漏洩先が団体の警告に応じないときは、裁判所に対し、漏洩した情報の使用差し止め仮処分を請求する。

### 第 39 条 （支援者への説明・謝罪）

（１）団体は、外部に漏洩した支援者情報の関係者に対し、次の事項を説明し、かつ謝罪する。

- ①漏洩した支援者情報の範囲

- ②漏洩先
- ③漏洩した日時
- ④漏洩した経緯、原因
- ⑤再発防止策の内容
- ⑥その他必要事項

(2) 支援者への説明と謝罪は、書面によって行う。

#### 第40条 (再発防止策)

(1) 情報管理一次責任者は、情報漏洩の原因について調査し、事故再発防止策を文書にて情報管理責任者に報告すること。(事故日から7 暦日以内)

(2) 情報管理責任者は、「事故再発防止策」を検討し、その結果を代表理事に報告し、承認を得る。(事故日から10 暦日以内)

(3) 情報管理責任者は、承認を受けた「事故再発防止策」を全スタッフに周知徹底させる。(事故日から14 暦日以内)

## 第七章 懲罰

#### 第41条 (懲戒処分等)

(1) 団体は、スタッフが秘扱情報・支援者情報の漏洩、紛失、減失、毀損、破壊及び不当なアクセス・使用・改ざん等にかかわったときは、そのスタッフを懲戒処分に付することができる。

(2) 前項において、団体は、そのスタッフを警察に告発することがある、また団体の被害甚大なる場合は、損害賠償請求することがある。

## 第八章 監査等

#### 第42条 (監査)

(1) 団体は、本規程に定める情報管理が適切に行われているかについて、少なくとも年一回、監査しなければならない。

(2) 前項の監査は、監事が実施し、代表理事に報告する。

(付則) この規程は、2012年6月14日から施行する。

2025年4月1日改定

別表

		保管方法等	
秘 扱 情 報	契約書等重要書類 賃貸契約書 認証関係書類 商標登録書類 保険証券類 銀行関係書類	①情報管理責任者がフォルダー等に収納し、金庫に保管して、常時施錠しておく。 ②情報管理一次責任者の許可が無い限りコピー禁止 ③情報管理一次責任者の了解を得ない者の取扱・閲覧禁止 ④持ち出し禁止 ⑤席を離れる時は格納する	
	極秘	紙媒体	
	人事ファイル 戦略ペーパー 分析データ 予算	電子データ	①フォルダーに必ずパスワードを設置する ②端末とサーバー等、複数個所に保存する ③原則持ち出し禁止 ④メールで送信する相手は情報管理責任者もしくは情報管理一次責任者とする ⑤情報管理一次責任者の指示が無い限りファイルコピー、電子メール送信、ファイル提供等は禁止 ⑥PCの画面に表示したまま席を離れない ⑦情報管理一次責任者の了解を得ない者の取扱・閲覧禁止
	団体外秘	紙媒体	①フォルダー等に収納し、不用意に訪問者の目に触れないようにする ②退出時は施錠できる場所に保管する ③持ち出し禁止 ④情報管理一次責任者の許可が無い限りコピー禁止 ⑤席を離れる時は格納する
	イベント企画 現地事業計画	電子データ	①フォルダーに必ずパスワードを設置する ②端末とサーバー等、複数個所に保存する ③原則持ち出し禁止 ④情報管理一次責任者の指示が無い限りファイルコピー、電子メール送信、ファイル提供等は禁止 ⑤席を離れる時はドキュメントを閉じる

支 援 者 情 報	重要帳票 複数の個人情報体系的に 整理された帳票		①フォルダー等に収納し、施錠可能なキャビネットあるいは引き出し等に保管し、常時施錠する。 ②コピーは情報管理一次責任者の許可がない限り禁止 ③持ち出し禁止 ④情報管理一次責任者の了解を得ない者の取扱・閲覧禁止 ⑤席を離れる時は格納する
	その他	紙媒体	
		電子データ	①フォルダーに必ずパスワードを設置する ②端末とサーバー等、複数個所に保存する ③クラウドへのアクセスは ID ごとに厳格に権限を設定する。 ④クラウドへのアクセスログを一定期間保存 ⑤原則持ち出し禁止 ⑥情報管理一次責任者の指示が無い限りファイルコピー、電子メール送信、ファイル提供等は禁止 ⑦席を離れる時は画面を閉じる ⑧情報管理一次責任者の了解を得ない者の取扱・閲覧禁止