個人情報の適切な管理

個人情報や、業務の中で知った秘匿すべき情報の取扱いに関する事故については、日常的な業務におけるちょっとした怠慢や不注意、出来心が、大きな被害につながります。
ほとんどの職員は、業務上個人情報等の秘密を扱う機会があることから、誰もが起こしうる不祥事の一つです。特に、電子データは、漏洩するとネット上で拡散される危険性があり、回収することは極めて困難です。事故防止のため、定められた手続きを各職員が遵守することはもちろん、手続き自体が形骸化しないよう、なぜそのような手続きが求められるのかを職員全員が意識し、相互に注意喚起できる組織的風土の醸成が求められます。

1　不祥事の事例

※この事例は実際にあった事案を参考に作成

事例１　教員 A は、自宅で仕事をするため、校長の許可を得ず、子供たちのテスト結果等が記録された USB メモリを職場から持ち出した。自家用車で退勤中、夕食のためにファミリーレストランに寄った際、USB メモリの入ったカバンを車内に置き去りにしたところ、車上荒らしに遭い、カバンごと USB メモリを盗まれた。

事例２　教員 B は、子供たちの健康状態に関する情報が記載された保健調査票を、普通教室の担任机の机上に置き忘れて帰宅した。翌朝、置忘れに気づいて慌てて教室を探したが、発見することは出来なかった。

事例３　教員 C は、担任している子供たちの写った写真を、個人名が分かる状態で、自身の SNS 上に掲載した。

2　組織的に不祥事を防ぐポイント

ポイント１　約束事の徹底

以下の約束事はどうなっていますか。

・個人情報を入手する方法（本人への許可、所属長への許可、使用目的の明示）
・個人情報の置き場所（データや紙の書類の保存方法、保管場所）
・個人情報を持ち出す際の手続き（持出し理由、事前許可）
・個人情報を持ち出した後の留意事項（携帯の方法、返却の際の手続き）

ポイント２　整理整頓

執務室や机上が散らかった状態では、容易に紛失事故が発生します。常に整理整頓を心掛け、書類や書籍などの置き場を決めましょう。

「気持ち」が散らかった状態も注意が必要です。あわてて複数の保護者に電子メールを送った際に、宛先を BCC にしなかったため保護者の連絡先が漏洩する事故が繰り返し起きています。個人情報を取り扱う際には、その重要性に留意し、落ち着いて処理をしましょう。

ポイント３　職員間の注意喚起

管理職は職員の情報の取扱いについて注意をする必要がありますが、管理職だけでは、大勢いる職員一人一人の対応に注意するには限界があります。

席の隣同士、学年団や各担当内の職員同士、互いに目を配らせ、不適切な取扱いがある場合には声かけを行い、学校（所属）全体で事故防止につなげましょう。

例えば、パソコンのパスワードをモニターに付箋で貼り付けている職員や、個人所有のパソコンやデジタルカメラ、USB メモリ等を業務に使用している職員はいませんか。

3　考えてみよう

①　個人情報等の取扱いに関する規程の内容について、職員に周知徹底されていますか。
②　個人情報等の取扱いが不適切な場合、直ぐに職員間で注意や是正ができていますか。
③　個人情報や秘匿すべき情報の管理・保管場所は所属所内で定められていますか。
④　自身の行動について、振り返ってみましょう。

□　自身が守るべき情報セキュリティの規定等を理解していますか。
□　自身が扱う情報について、どれが個人情報又は秘匿すべき情報か把握していますか。

□　個人情報（通知表や実施したテスト用紙などの成績物等）や秘匿情報が記載された文書等を、教室（又は執務室の机上）に置きっぱなしにいていることはありませんか。
□　個人情報や USB メモリ等電子的記録媒体を、やむを得ず持ち出す場合、所属長（校長）の許可を得ていますか。
□　許可を得てやむを得ず個人情報等が記載された紙や USB メモリ等電子的記録媒体を持ち出した場合、常に盗難・紛失に注意を払いつつ携帯するとともに、他の場所に立ち寄ったりせず速やかに帰宅していますか。
□　持ち出した個人情報等は許可された期限までに返却する、貸与された USB メモリ等に保存したデータを削除するなど決められた事後の手続きを確実に行っていますか。
□　個人情報を利用目的以外に使用していませんか。
□　個人情報を本人の同意を得ずに第三者に提供していませんか。
□　私的な手帳などに児童・生徒等の個人情報を書き込んで持ち歩いていませんか。
□　飲食店や公共の場所などで、子どもや保護者のこと（業務で知り得た情報）を話題にすることはありませんか。
□　個人のブログやＸ（旧Ｔｗｉｔｔｅｒ）、インスタグラム、ＬＩＮＥなどのＳＮＳを使って、個人情報や秘匿情報にあたる写真や内容を投稿したり、特定の人へ送信したりしていませんか。
□　端末の故障や誤操作等によるデータの滅失・毀損に備え、必要に応じてバックアップをとっていますか。
□　作業後の個人情報のデータは、定められた場所に保存するか、削除していますか。
□　ハードディスクやＣＤ、ＤＶＤ、ＵＳＢメモリ等を廃棄する場合、データ消去だけでなく、情報漏洩防止の対策（専用ソフトの使用や物理的破壊等）を施していますか。
□　保護者や外部の業者など複数の相手にメールを送信する場合は BCC で送付していますか。また、送信する前に送信先及び内容に誤りや不適切な点がないか複数の目で確認していますか。

4　問われる責任

（1）行政上の責任・・・懲戒処分（減給又は戒告）　（2）刑事上の責任・・・懲役、罰金等
（3）民事上の責任・・・損害賠償等　（4）社会的な責任・・・報道等

【参考】

懲戒処分の基準　第２　１（９）個人情報の盗難、紛失又は流出

過失により個人情報を盗まれ、紛失し、又は流出させ、公務の運営に支障を生じさせた職員は、減給又は戒告とする。この場合において、公務の運営に重大な支障を生じさせた職員は、停職又は減給とする。

地方公務員法　第３４条　秘密を守る義務

職員は、職務上知り得た秘密を漏らしてはならない。その職を退いた後も、また、同様とする。

個人情報の保護に関する法律　第 180 条

教育委員会の職員又は職員であった者等が、その業務に関して知り得た保有個人情報を自己若しくは第三者の不正な利益を図る目的で提供し、又は盗用したときは、１年以下の懲役又は５０万円以下の罰金に処する。

コラム

黒塗りの方法、大丈夫？

【事例】

個人情報にマスキング（黒塗り）をした電子ファイルをウェブサイトに掲載したところ、特定の環境下でマスキングが外れ、マスキングされた内容が閲覧可能になった事例がありました。

【原因】

正しいマスキング方法によらず、マスキング処理を行ったことが原因です。

【防ぐためには】

電子ファイルを画像形式にするなど、マスキング部分がいかなる操作等によっても閲覧できない処理が必要です。今一度、黒塗りの方法について確認してみましょう。

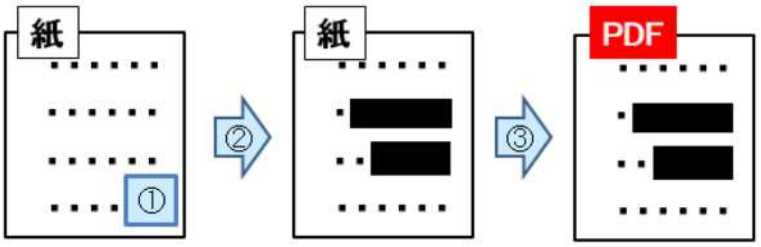
（次頁「不開示情報を含む行政文書等を電子的に開示する際の墨塗り処理の方法」参照）

◆　不開示情報を含む行政文書等を電子的に開示する際の墨塗り処理の方法

出典：　個人情報の保護に関する法律についての事務対応ガイド（個人情報保護委員会）を加工して作成　https://www.ppc.go.jp/personalinfo/legal/

1　電磁的記録の提供により開示しようとする行政文書等が紙の文書のとき

コピー（写し）を用意し、そのコピー（写し）の不開示にしようとする部分に墨塗り処理を行い、これをスキャナで読み取って電磁的記録（PDF ファイル）とし、当該電磁的記録を開示する。

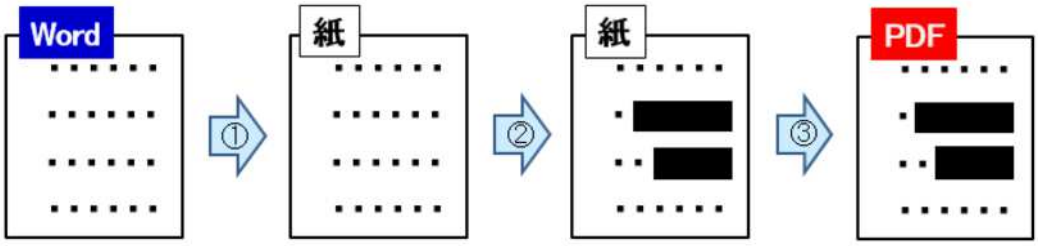


① 行政文書のコピー（写し）を用意
② 不開示にしようとする部分を墨塗り（例：マジックペン等で塗り潰し）
③ スキャナで読み取って電磁的記録化（PDFファイル）

なお、不開示にしようとする部分に墨塗り処理を行った後、当該部分が判読できる状態になっていないか目視で確認することが必要である。

2　電磁的記録の提供により開示しようとする行政文書等が電磁的記録のとき

一度、プリントアウトして紙媒体とした上で、不開示にしようとする部分に墨塗り処理を行い、これをスキャナで読み取って再び電磁的記録（PDF ファイル）とし、当該電磁的記録を開示する。

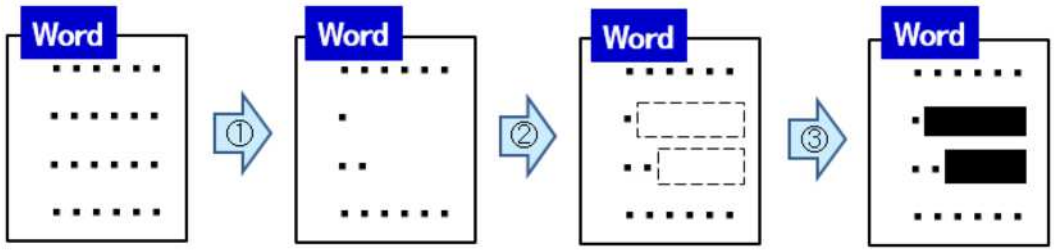


① 行政文書をプリントアウトして紙媒体を用意
② 不開示にしようする部分を墨塗り（例：マジックペン等で塗り潰し）
③ スキャナで読み取って電磁的記録化（PDFファイル）

なお、不開示にしようとする部分に墨塗り処理を行った後、当該部分が判読できる状態になっていないか目視で確認することが必要である。

３　その他に考えられる方法

電磁的記録の不開示にしようとする部分の情報（文字等）を削除し、黒く塗り潰したテキストボックスを置いた上で、当該電磁的記録を開示する。

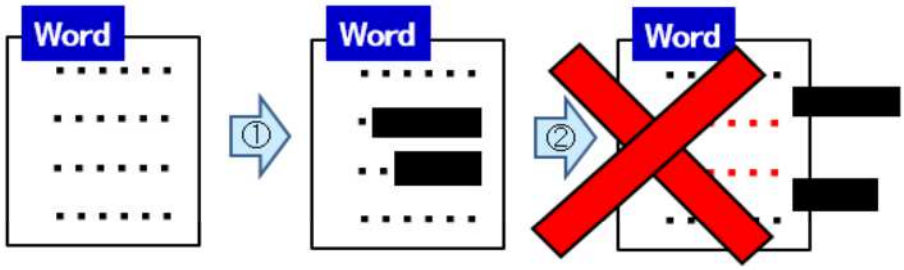


① 不開示にしようとする部分の情報（文字等）を削除
② 不開示にしようとする部分がどこか目視で把握可能にするため、削除した文字数分空白を入力
③ 当該空白の上に黒く塗り潰したテキストボックスを置く
（Excelファイルでは、セルを黒く塗り潰す）

なお、不開示にしようとする部分の情報（文字等）を削除した後、「変更履歴の記録」機能により、当該情報が判読できる状態になっていないことを目視で確認することが必要である。

４　不適切なマスキングの例

上記３の例で、不開示部分の情報を削除することなく、単に、当該部分に黒く塗りつぶしたテキストボックスを置くだけでは、その後に当該テキストボックスを容易に外すことが可能であり、不開示部分のテキストデータが保持されているため、マスキング処理の方法としては不十分である。



① 不開示にしようとする部分の情報（文字等）を削除せずに黒く塗り潰したテキストボックスを置く
② テキストボックスをずらしたり削除したりすることで、不開示情報を確認することができる

１～３以外のマスキング方法については、国の機関である個人情報保護委員会作成の「個人情報の保護に関する法律についての事務対応ガイド」等を参照してください。