

県立学校における電子情報保全に関する ガイドライン

平成21年6月改定

熊本県教育委員会

目次

1	このガイドラインの趣旨及び対象者	3
2	情報セキュリティ管理体制	3
3	電子情報を利用する場合の基本的な注意事項	4
	(1) 遵守義務	4
	(2) 守秘義務	4
	(3) 目的外利用の禁止	4
	(4) 権限がある者のみが行うこと	4
	(5) 非常勤職員及び臨時職員等への周知	4
4	特に重要な情報の管理	5
5	電子個人情報を取り扱う際の注意点	5
	(1) 個人情報の取得	5
	(2) 第三者提供	5
	(3) オンライン結合による提供	6
	(4) 廃棄	6
	(5) 委託先の監督	6
6	端末、ソフトウェア及び記録媒体の取扱い	7
	(1) 端末及び記録媒体を取り扱う際の注意点	7
	(2) 個人所有端末の利用	8
	(3) 情報資産の持ち出し	8
	(4) ネットワーク管理	9
	(5) 不正アクセスの禁止	9
7	パスワードの管理	9
8	電子メール利用上の注意	9
9	インターネット利用上の注意	10
10	コンピュータウイルス対策	10
	(1) コンピュータウイルスとは	10
	(2) ウィルス対策	10
11	緊急事態時の対応	11
	(1) 緊急事態とは	11
	(2) 緊急事態時の報告	11
	(3) ウィルス感染時の報告	12
12	情報流出時の対応	13
	(1) 事故の発見	13
	(2) 校長への報告	13

(3)	本人への通知	14
(4)	事故が生じたことの公表	14
(5)	その他の措置	15
(6)	教育政策課との協議、てん末の報告	15
13	懲戒	15
14	外部ホームページ公開時の対策	16
15	様式集.....	16
16	結び.....	16

1 このガイドラインの趣旨及び対象者

このガイドラインは、県立学校における熊本県教育・文化ネットワーク及びその他の電子情報の取扱いに関し、児童・生徒の個人情報の保護、情報資産*1の保全など電子情報の適正な取扱いを確保するために校長及び教職員が取るべき措置について定めるものである。

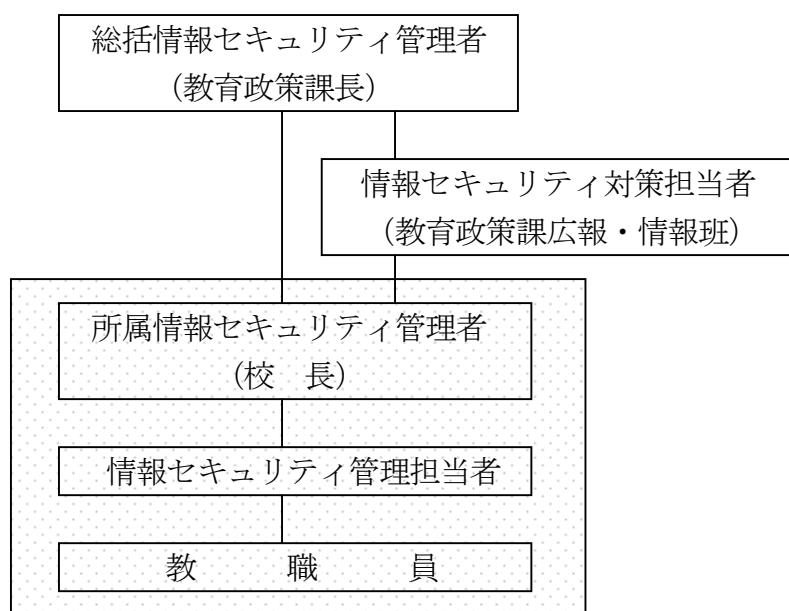
校長及びすべての教職員（非常勤職員、臨時職員を含む。以下「教職員」という。）は、このガイドラインに従って電子情報を取り扱うものとする。

2 情報セキュリティ管理体制

県立学校における情報セキュリティ対策は次に掲げる体制により行う。

校長は、所属情報セキュリティ管理者として、学校における電子情報の適正な運用管理を行うこと。また、所属職員のうち情報セキュリティに関する知識と経験を有する者を情報セキュリティ管理担当者として選任すると共に情報セキュリティ管理担当者及び教職員に対し、その責務の重要性を認識させ、具体的な個人データの保護措置に習熟させるため、必要な教育及び研修を行うこと。

情報セキュリティ管理担当者は、児童・生徒等に関する電子情報（以下「電子個人情報」という。）の運用管理やネットワークの保全を行う。なお、情報セキュリティ管理担当者の運用管理が広範に及ぶ時は、情報セキュリティ管理担当者を複数設置して事務を分担させることができる。



※網掛け部がこのガイドラインの対象者の範囲

*1情報資産とは、コンピュータや記録媒体に記録された情報や情報を取り扱うコンピュータやネットワークなどの情報システムのことをいう。

3 電子情報を利用する場合の基本的な注意事項

(1) 遵守義務

教職員は、以下の法令、条例及びこれに関連する規定を遵守すること。

- ア 熊本県個人情報保護条例
- イ 著作権法
- ウ 不正アクセス行為の禁止等に関する法律

(2) 守秘義務

教職員は、電子情報を利用するに当たっては、職務上知り得た秘密を漏らしてはならないこと等を定めた地方公務員法第34条の規定に留意すること。

例として、以下のような情報の取扱いについては特に注意が必要である。

- ア 児童・生徒の個人情報
- イ 保護者など児童・生徒以外の者の個人情報
- ウ 指導要録・調査書、学力検査に関わる情報等

(3) 目的外利用の禁止

教職員は、学校において、情報資産及びコンピュータを職務遂行以外の目的に使用してはならない。例示すれば以下のとおりである。

- ア 職務に必要なでない情報資産を使用しないこと
- イ 職務に関係のない者に対して情報資産の提供を行わないこと
- ウ 職務に関係のないソフトウェア等をダウンロードしないこと
- エ 職務に関係のないファイル共有ソフトウェア等をインストールしないこと

(4) 権限がある者のみが取り扱うこと

児童・生徒等に関する電子個人情報の安全管理のため、電子個人情報の取扱いについては、権限を与えられた者のみが業務の遂行上必要な限りにおいて取り扱うこと。

(5) 非常勤職員及び臨時職員等への周知

校長は、非常勤職員及び臨時職員の配属の際、このガイドラインを周知し、遵守させなければならない。なお、教育実習生についても同様とする。

4 特に重要な情報の管理

校務情報のうち下記に掲げるものについては、特に厳重な運用管理を行うこと。

- ア 熊本県個人情報保護条例（平成16年熊本県条例第67号）に規定する個人情報
- イ 法令又は条例の定めにより守秘義務を課されている行政情報（上記個人情報以外のもの）
- ウ 漏えいした場合、学校運営に対する信頼を著しく害するおそれのある情報
- エ 滅失し、又はき損した場合、その復元が著しく困難となり、教育活動等の円滑な推進を妨げる恐れのある校務情報
- オ 情報システムに係るパスワード及びシステム設定情報

5 電子個人情報を取り扱う際の注意点

熊本県個人情報保護条例第2章第1節「実施機関の義務」では、個人情報を取り扱う際に遵守すべき事項が定められている。これらの規定は電子情報の形で個人情報を取り扱う際にも適用されるものであり、学校において電子個人情報を取り扱うに当たっては常に参照する必要がある。

その主な事項は次のとおりである。

(1) 個人情報の取得（条例第6条、第7条）

ア 利用目的の明確化

個人情報を取得する場合は、あらかじめその利用目的を具体的に明確にすることが必要。

イ 利用目的の明示

個人情報は、その本人から収集することが原則である。本人から書面（電磁的記録を含む）により個人情報を収集するに当たっては、当該本人に当該個人情報の利用目的を明示しなければならない。ただし、状況から見てその情報を収集する目的が明らかな場合など、明示する必要がない場合もある。

(2) 第三者への提供（条例第8条、第12条）

児童・生徒に関するものを始めとして、電子個人情報は原則として本来の目的以外のために利用すること、又は第三者に提供することはできないことに留意すること（条例第8条第1項）。本人の同意がある場合など一定の場合には第三者への提供が可能である（同条第2項）が、その場合も、同条例第12条に基づき、提供を受ける者が、例えば、以下のような措置を講ずるよう文書で指示すること。

- ア 提供先において、その従業者に対し当該電子個人情報の取扱いを通じて知り得た個人情報を漏らし、又は盗用しないことを徹底すること
- イ 当該電子個人情報の第三者への再提供は原則として行わないこと。ただし、真に必要な場合には、学校長の下承を得ること
- ウ 提供先における保管期間等を明示すること
- エ 利用目的達成後の電子個人情報の返却又は提供先における破棄若しくは削除を適切かつ確実にを行うこと
- オ 提供先における電子個人情報の複写及び複製は行わないこと（安全管理上必要なバックアップを目的とするものを除く）

(3) オンライン結合による提供（条例第9条）

オンライン結合（通信回線を用いて学校が管理するコンピュータ等と学校以外が管理するコンピュータ等を接続し、学校の保有する個人情報を学校以外のものが随時入手し得る状態にする方法）により、個人情報を学校以外のものへ提供してはならない。ただし、学校のホームページによる情報提供については、条例第9条第2項の例外規定により、熊本県個人情報保護制度審議会から、氏名、性別、学校名、学年、学級、クラブ活動の状況等を公開することについては承認を得ているが、これらの範囲を超えないように留意すること。

なお、学校のホームページに個人情報を掲載しようとするときは、熊本県教育情報システム運用要項も参照のうえ、次に掲げる事項を遵守すること。

- ア ホームページへの掲載については、本人の承諾を得ること
- イ 氏名については、フルネームでの表記をしないこと
- ウ 写真については、個人が特定できないように配慮すること
- エ プライバシーに関わる事項は掲載しないこと

(4) 廃棄（条例第10条第3項）

保有する必要のなくなった電子個人情報は、原則として確実かつ速やかに廃棄又は消去すること。

(5) 委託先の監督（条例第13条）

児童・生徒のスポーツテストや模試等の電子個人情報を取り扱う事務を外部委託するに当たっては、「熊本県個人情報取扱事務委託基準」を遵守すること。

また、その契約において、委託を受ける者が個人情報保護のために講ずべき措置を明示すること。具体的な措置としては、以下のようなことが考えられる。

- ア 委託先において、その従業者に対し当該個人データの取扱いを通じて知り得た個人情報を漏らし、又は盗用してはならないこと

- イ 当該個人データの取扱いの再委託を行うに当たっては、学校へその旨文書をもって報告することウ 委託先の責任者、委託内容、作業者、作業場所、委託契約期間等を明記すること
- エ 提供された電子個人情報の目的外利用及び受託者以外の者への提供を禁止すること、又、利用目的達成後の電子個人情報の返却又は委託先における破棄若しくは削除が適切かつ確実になされること
- オ 委託先における電子個人情報の加工（委託契約の範囲内のものを除く。）、改ざん等を禁止し、又は制限すること
- カ 委託先における電子個人情報の複写又は複製（安全管理上必要なバックアップを目的とするもの等委託契約範囲内のものを除く。）を禁止すること
- キ 委託先において電子個人情報の漏えい等の事故が発生した場合における委託元への報告義務を課すこと
- ク 委託先において電子個人情報の漏えい等の事故が発生した場合における委託先の責任が明確化されていること
- ケ 必要がある場合は、委託先における電子個人情報の状況について随時実地に調査できること

6 端末^{*2}、ソフトウェア及び記録媒体の取扱い

(1) 端末及び記録媒体を取り扱う際の注意点

- ア 校長は、学校における端末やソフトウェア等を適切に管理しなければならない。
 - (ア) 学校における端末のネットワークアドレスを管理し、ネットワークアドレスの付与・変更があった場合は、様式1「校内ネットワークアドレス一覧」により、教育政策課長に報告すること
 - (イ) 導入したソフトウェアの管理を適正に行い、ライセンス・著作権法違反（違法な複製等）が生じないようにすること
- イ 教職員は、使用する端末等や記録媒体が、許可なく第三者に使用されること、又は情報を閲覧されることがないように、以下のような措置を講ずること。
 - (ア) 電子個人情報を扱う端末は、第三者の目に触れにくい場所に設置すること
 - (イ) 記録媒体は、キャビネットや脇卓等の施錠可能な場所に保管すること
 - (ウ) ネットワークを利用し、電子個人情報を共有する場合は、アクセス権の設定を行い、その事務を処理する権限のある者のみが電子個人情報を取り扱うこと

^{*2} 端末とは、パソコンなどの情報端末をいう。

- (エ) 盗聴等を防止するため、原則として無線LANは使用しないものとするが、やむをえず無線LANを使用する場合は、MACアドレス等によるユーザ管理（ユーザ制限）を行い、通信については暗号化を行うこと
- (オ) 電子個人情報を扱う端末は、パスワードの設定を行い、第三者の利用を防ぐこと
- (カ) 教職員は、長時間離席する際は、端末の電源を切るなどの措置を講じること
- ウ 校長は、端末等の盗難や第三者のアクセス防止などのため、職員室等に教職員がいない場合の施錠管理を徹底すること
- エ 教職員は、端末等の盗難を防ぐため、次に掲げるいずれかの事項を実施するよう努めなければならない。
 - (ア) セキュリティロック等による机への固定を行うこと
 - (イ) 長時間の離席時や帰宅時は、キャビネットや脇卓等の施錠可能な場所に保管すること

(2) 個人所有端末の利用

- 教職員は、個人所有端末を学校で使用する場合は、校長への届出をし、ネットワークアドレスの付与を受けなければならない。
- ア 個人所有端末には、必ずウィルス対策ソフトウェアを導入すること
 - イ 職務に関係ないファイル共有ソフトウェア等を導入しないこと
 - ウ 電子個人情報はサーバや記録媒体に保存することとし、個人所有端末には保存しないこと

(3) 情報資産の持ち出し

- ア 教職員は、情報資産を設置場所以外の場所へ持ち出す場合は、校長の許可を得なければならない。
 - (ア) 電子個人情報が保存された記録媒体及び端末を設置場所以外へ持ち出す場合は、第三者に読み取られないよう暗号化するなどセキュリティの向上に努めること
 - (イ) 持ち出した情報資産をファイル共有ソフトウェアがインストールされたパソコンで取り扱わないこと
 - (ウ) 万一、盗難や紛失により、電子個人情報等が流出した場合は、速やかに校長に報告すること
- イ 校長は、管理する端末が全て適切な場所にある事を確実にするため、定期的な点検等に努めなければならない。
 - (ア) 端末等の保管状況の調査を行うこと

(イ) 最新のウィルス対策ソフトウェアが導入されているか調査を行うこと

(4) ネットワーク管理

教職員は、端末等の利用において、次に掲げる事項を遵守すること。

- ア 端末等を無断で増設又は改造してはならない
- イ 端末等に無断でソフトウェアを導入、変更又は消去してはならない
- ウ 端末等のネットワーク接続設定などを無断で変更してはならない
- エ ダイアルアップなどを使用して、無断で熊本県教育・文化ネットワーク以外のネットワークに接続してはならない
- オ VPNソフトウェアを使用して、熊本県教育・文化ネットワークに接続してはならない
- カ 個人端末を外部から持ち込み、無断でネットワークに接続してはならない

(5) 不正アクセスの禁止

教職員は、以下のような不正アクセス又はそれに類する行為を行ってはならない。

- ア 他人の ID を利用して不正にデータにアクセスすること
- イ 私的関心など業務以外の目的でデータにアクセスすること
- ウ ネットワークを経由して他のコンピュータに許可なく侵入すること

7 パスワードの管理

教職員は、パスワードの管理について、次の事項を遵守すること。

- ア パスワードを他人に使用させないこと
- イ パスワードを公にしないこと
- ウ 初期値として設定されているパスワードを使用しないこと
- エ パスワードを定期的に変更すること
- オ 過去に使用したパスワードは極力使用しないこと
- カ パスワードの入力を省略できる機能を使用しないこと
- キ パスワードを入力する場合は、第三者に覗き見られないように注意すること
- ク パスワードを失念した場合、及び他人に知られた恐れのある場合は、直ちに校長に届け出ること
- ケ 他人のパスワードを使用しないこと

8 電子メール利用上の注意

教職員は、電子メールの利用において、次に掲げる事項を遵守すること。

- ア 個人情報を含む電子メールを私的に所有するメールアドレスに転送しない

こと

- イ 電子メールの発信時には、送信相手が正規の送信相手か否かを確認すること
- ウ 電子メールの添付ファイルは、送信前又は受信後にウィルス検査を行うこと
- エ チェインメール（不幸の手紙の電子メール版など）やジャンクメール（全く意味のない電子メール）は、転送しないこと
- オ 不特定多数に向けて無作為に送信しないこと
- カ 実行形式のファイル（拡張子が「.EXE」のファイル）を添付しないこと
- キ 緊急やむを得ない場合は別として、児童・生徒等に関するものを始めとする個人情報や外部に送信しないこと
- ク 他人のプライバシーに関する内容を送信しないこと
- ケ 他人を誹謗・中傷するような内容を送信しないこと
- コ 公序良俗に反する内容を送信しないこと
- サ 不審な者からの電子メールは、開かず削除すること
- シ 外部の複数人にメールを送信する際はBCCを利用すること

9 インターネット利用上の注意

教職員は、インターネットの利用において、次に掲げる事項を遵守すること。

- ア 職務上必要のないサイトを閲覧しないこと
- イ 職務上必要のない掲示板への書込みをしないこと
- ウ 職務上必要のないソフトウェアや楽曲等をダウンロードしないこと

10 コンピュータウィルス対策

(1) コンピュータウィルスとは

コンピュータウィルスは他人のコンピュータシステムやデータ等の破壊を目的として作られた特殊なプログラムであり、コンピュータウィルスが埋め込まれた電子メールやホームページを閲覧したり、ファイルを共有することによって感染する。また、多くのコンピュータウィルスが自分自身を複製する機能を持ち、次々と増殖する仕組みを持つ。

ウィルス感染の兆候の例

- パソコンが勝手に再起動を繰り返す
- パソコンの動作がいつもより異常に遅い
- 画面上に見知らぬメッセージがいきなり現れた
- 保存していたはずのファイルがなくなっている
- 作成していないはずのファイルが作成されている など

(2) ウィルス対策

ア 校長は、すべてのコンピュータにウィルス対策ソフトウェアを導入すること。

イ 校長は、導入したウィルス対策ソフトウェアを常に最新の状態に保つこと。

ウ 教職員は、ウィルスの感染を防止するため、次に掲げる事項を遵守すること。

(ア) ウィルス対策ソフトウェアを常時起動しておくこと

(イ) ウィルス対策ソフトウェアのバージョン及び定義ファイルが常に最新の状態に保たれているか確認すること

(ウ) フロッピーディスクなど外部記録媒体を使用してファイルを持ち出し又は持ち込む場合は、その外部記録媒体のウィルス検査を行うこと

1.1 緊急事態時の対応

(1) 緊急事態とは

緊急事態とは、所属組織において発生する情報セキュリティに対する侵害の発生又はその可能性のある場合であり、障害・事故・災害を総称する。

ア 障害 機器故障等によるシステム又はネットワークの停止

イ 災害 地震・台風・落雷・火災などによって引き起こされる被害

ウ 事故 障害・災害以外の緊急事態（ウィルス感染、情報流出、紛失・盗難等）

(2) 緊急事態時の報告

ア 教職員は、緊急事態の発生時に、その証拠保全のため現状の維持に努めるとともに、速やかに次に掲げる事項を校長又は情報セキュリティ管理担当者に報告すること。なお、ウィルス感染については(3) ウィルス感染時の報告、情報流出については1.2 情報流出時の対応による。

(ア) 発生日時又は検知日時

(イ) 発見者

(ウ) 情報セキュリティ侵害を受けた対象

(エ) 緊急事態の概要

(オ) 実施済の応急処置

(カ) 被害の有無及び影響範囲

(キ) 発生原因

イ 校長は、報告のあった緊急事態について、速やかに教育政策課に報告するとともに、その指示に従い必要な措置を講ずること。

また、緊急事態の概要が把握できた時点で、教育政策課長へ様式2「緊急

事態報告書兼回復報告書」により報告すること。

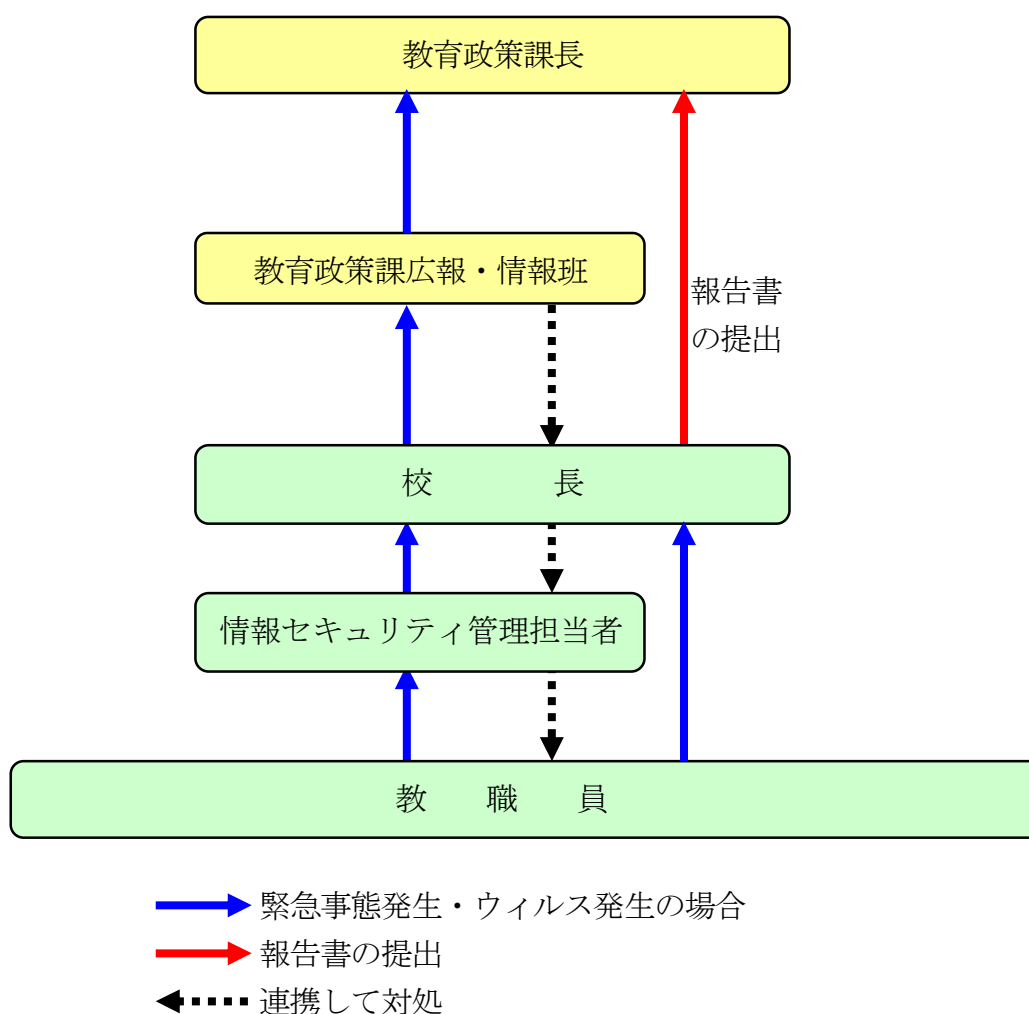
(3) ウィルス感染時の報告

ア 教職員は、ウィルスに感染又は感染の疑いがある場合には、該当する端末を速やかにネットワークから切り離し、校長又は情報セキュリティ管理担当者に報告すること。

イ 校長は、ウィルスに感染又は感染の疑いが生じた場合には、速やかに教育政策課に報告するとともに、協議して必要な回復措置を講ずること。

また、ウィルス感染の概要が把握できた時点で、教育政策課長へ様式3「コンピュータウィルス感染報告書兼回復報告書」により報告すること。

緊急事態時の連絡体制



1 2 情報流出時の対応

電子個人情報や個人情報が記録された書類の流出、紛失等の事故が生じた場合（事故が生じたのではないかとの疑いを抱いた場合を含む。）は、次の手順を参考に対応する。

(1) 事故の発見

事故を発見する契機としては、主に次の3つの場合が考えられる。

ア 事故を起こした当事者からの報告

例：個人情報記録された書類を教職員本人が紛失した場合

イ 当事者以外の教職員からの報告・内部通報

例：業務の委託先又は特定の教職員から電子個人情報が流出していることを教職員が発見した場合。なお、ファイル共有ソフトウェア使用などの教職員の非違行為については、公益通報制度の利用も考えられる。

ウ 県民など外部からの通報

例：県民から学校の個人情報が流出しているのではないかと問い合わせがあった場合

イ、ウの場合、通報を受けた者は、以下の事項について、通報者からできるだけ詳しく聴取する。

- ① 通報者の氏名、住所及び連絡先（匿名で受けることもあり得る。）
- ② 事故により流出した個人情報の項目（氏名、住所、電話番号、成績等）
- ③ 事故の概要及び経緯
- ④ 個人情報が流出しているのではないかと疑いを抱いた理由

(2) 校長への報告

事故を発見した者もしくは通報を受けた者は、事故の概要等について、速やかに校長へ報告する。

校長は、報告を受けた事故について、必要に応じて、事実確認、調査等を行い、以下の点について整理を行うとともに教育政策課広報・情報班へ報告する。

ア 事故の内容及びその原因（又は原因と考えられるもの）

イ 事故が生じたと断定できない場合は、その事故の可能性の程度

ウ 事故の規模

事故により個人情報が流出したことが確認できた者及び確認はできないがその可能性が否定できない者（以下「本人」という。）の人数、範囲等

エ 事故により流出した個人情報の項目及びその重要度

- ① 氏名、住所、性別等の基本的な（個人識別のための）情報

- ② 成績、指導歴等の重要度の高い情報
- オ 事故が生じた時期（又は生じたと考えられる時期）
- カ 事故への対応策
 - ① 流出した個人情報の検索、回収等の方針
 - ② 犯罪性が認められる場合は、被害届の提出及び告訴等の判断
 - ③ 本人への対応
- キ 個人情報の管理体制の見直し及び再発防止策

(3) 本人への通知

- ア 通知の目的・意義
事故についての謝罪と二次被害を防止するための注意喚起のために行う。
- イ 通知すべき主な内容
 - ① 判明している事実関係
 - ② 謝罪
 - ③ 二次被害を防止するための注意喚起
 - ④ 今後の対応策
 - ⑤ 問い合わせ窓口
- ウ 通知の時期
事故が生じた可能性があるとして判断した時点で行う。
- エ 通知の方法
口頭又は文書による通知など、適当と認められる方法により行う。
本人の数が多く、又は本人と連絡がとれないなど、個別的な通知が困難である場合は、これに代えて、記者発表、ホームページへの掲載等により周知する。

(4) 事故が生じたことの公表

- ア 公表の目的・意義
本人への個別的な周知に代わる措置だけでなく、広く県民に対して事実関係を公表することにより、類似事案の発生を回避するとともに、学校として説明責任を果たすために行う。
- イ 公表の目安
一般に、以下のような場合に、公表する必要があると考えられる。
 - ① 本人へ個別的に通知することが困難である場合
 - ② 本人へ個別的に通知だけでなく、類似事案の発生回避の観点から、県民に周知する必要があると認められる場合
 - ③ 学校として説明責任を果たし、学校の適正な運営と透明性を確保する観点から、公表する必要があると認められる場合

ウ 公表すべき主な内容

「(3) 本人への通知 イ 通知すべき主な内容」を参照。

本人へ通知を行っている場合はその旨、個人情報の管理体制の見直し、再発防止策の状況等を考慮しながら、個別的に判断する。

エ 公表の時期

事故についての事実確認、調査等の進捗状況、個人情報の管理体制の見直し、再発防止策の状況等を考慮しながら、個別的に判断する。

なお、本人への個別的な通知に代えて公表を行う場合は、事故が生じた可能性があると判断した時点で行う。

オ 公表の方法

記者発表、ホームページへの掲載等

(5) その他の措置

ア 損害賠償の請求

本人から損害賠償の請求があった場合、個人情報を流出させた委託先又は個人情報を漏えいした行為者に対して損害賠償の請求を行う場合は、法的な責任の有無について検討する。

なお、学校の過失が明らかな場合は、教育政策課広報・情報班と相談のうえ対応する。

イ 委託契約に基づく措置等

業務の委託先から個人情報が流出させた場合は、委託契約に基づく措置のほか、契約条項の見直し、又は契約自体を解除すべきかどうかを検討する。

(6) 教育政策課との協議、てん末の報告

個人情報流出等の事故の対応に当たっては、必要に応じて教育政策課広報・情報班と協議するとともに、事故のてん末について報告する。

1.3 懲戒

このガイドラインに違反した教職員及びその校長は、その重大性、発生した事案の状況などを斟酌し、地方公務員法及び関係規定による懲戒処分の対象とする。

14 外部ホームページ公開時の対策

校長は、外部に公開しているシステムへ情報を公開する際には、個人情報保護や著作権保護等を確実にを行うため、複数の職員に内容の確認を行わせなければならない。

15 様式集

様式 No	様式名称	用途
様式1	校内ネットワークアドレス一覧	校内のネットワークアドレスを届け出る場合
様式2	緊急事態報告書兼回復報告書	緊急事態発生の場合（ウイルス感染被害を除く）
様式3	コンピュータウイルス感染報告書兼回復報告書	ウイルスに感染又は感染の疑いが生じた場合またはウイルス感染から回復した場合
参 考	個人所有端末ネットワーク接続許可願	個人所有端末を校内ネットワークに接続する場合
参 考	情報資産学校外持ち出し許可願	情報資産を学校外へ持ち出す場合

16 結び

学校では、多くの個人情報を取り扱っていますが、特に電子情報については、短時間に大量の情報を処理できる反面、ネットワークによる情報の共有や小型の記録媒体に大量の情報を入れて持ち運びできるなど、取扱いについては特に注意をしなければならないこともあります。このガイドラインの内容を心に留め、電子情報を適正に活用して、校務の効率化、児童・生徒へのよりきめ細かな対応など、より質の高い教育を目指しましょう。

様式2

〇〇第 号
平成 年 月 日

総括情報セキュリティ管理者 様
(教育政策課長)

熊本県立〇〇〇〇学校長
〇 〇 〇 〇

緊急事態報告書兼回復報告書

報告元 (発見者)	所属 職・氏名 電話番号： メールアドレス：
緊急 事態 報告	発見日時 平成 年 月 日 午前・午後 時 分
	侵害を受けた対象
	緊急事態の概要 <input type="checkbox"/> 障害 <input type="checkbox"/> 災害 <input type="checkbox"/> 事故 概要：
	応急処理内容 (一次対処)
	被害の有無及び影響範囲 (画面メッセージ、ログ等の 被害記録等) <input type="checkbox"/> 被害発生無 <input type="checkbox"/> 被害発生有 影響範囲：
	発生原因 (想定される原因)

回復 報告	回復措置内容
	回復日時 平成 年 月 日 午前・午後 時 分頃

様式3

〇〇第 号
平成 年 月 日

総括情報セキュリティ管理者 様
(教育政策課長)

熊本県立〇〇〇〇学校長
〇 〇 〇 〇

コンピュータウイルス感染報告書兼回復報告書

報告元 (発見者)		所属 職・氏名 電話番号： メールアドレス：	
感 染 報 告	発見日時	平成 年 月 日 午前・午後 時 分	
	発見状況等	ウイルス名： 発見状況等：	
	応急処理内容(一次対処)		
	被害の有無及び影響範囲 (画面メッセージ、ログ等の 被害記録等)	<input type="checkbox"/> 被害発生無 <input type="checkbox"/> 被害発生有 影響範囲：	
	感染経路 (なぜ感染したか)		
	感染端末等	OS	
使用目的			
ウイルス 対策ソフト			
定義ファ イル			
回 復 報 告	回復措置内容		
	回復日時	平成 年 月 日 午前・午後 時 分頃	

(参考)

個人所有端末ネットワーク接続許可願

平成 年 月 日

熊本県立〇〇〇〇学校長
〇 〇 〇 〇 様

職 名
氏 名 印

下記の個人所有端末を校内ネットワーク（熊本県教育・文化ネットワークを含む）に接続したく、許可下さるようお願いします。

記

- 1 接続端末（メーカー名、型番）
- 2 ドメイン名（ワークグループ名）
- 3 コンピュータ名
- 4 MACアドレス
- 5 IPアドレス（*付与側で記入）

(参考)

情報資産学校外持ち出し許可願

平成 年 月 日

熊本県立〇〇〇〇学校長
〇 〇 〇 〇 様

職 名
氏 名 印

下記の情報資産を学校外に持ち出しいたしたく、許可下さるようお願いいたします。

なお、持ち出した情報資産を取り扱う場合は、ファイル共有ソフトウェア（Winny等）がインストールされた端末等で取り扱わない、ウィルス対策ソフトウェアをインストールし、かつ、最新の状態にした端末等で取り扱うなど、十分なセキュリティ対策を講じたうえで取り扱います。

記

- 1 情報資産の名称
- 2 記録媒体
- 3 学校外へ持ち出す目的
- 4 持ち出し期間
- 5 持ち出し場所

注意：電子個人情報の学校外持ち出しは原則禁止。

許可を受け、持ち出す場合は、暗号化を行うこと。また、紛失等の事故のないよう管理は厳重に行うこと。