

情報セキュリティに関するリスクを回避して、 トラブルなく安全に情報を活用をするために、 学校情報セキュリティポリシーを遵守しましょう！

情報リスクとは、情報を扱う中で、危険に遭う可能性や損をする可能性のこと。
その中で、

怖いのは、やはり**個人情報**の漏洩！

本県における
過去の事例

■万が一情報漏洩が起きたら
【民事責任】 【刑事責任】 【行政責任】

民事賠償

刑事罰

信用失墜

- 個人情報FAX誤送信
- PC盗難
- ウィニー通じ名簿流出
- 児童情報WEB掲載
- 通知票盗難
- ネット地図に個人名流出
- USBメモリ紛失



これら情報漏洩に共通する原因は、
情報資産の持ち出し、ネットに発信する際の危機感の欠如、責任感不足等です。
教職員一人一人が心がけるべき事項を示す「学校情報セキュリティポリシー」について、
点検し、遵守することが、被害者だけではなく、加害者になることを防ぎます。

今すぐできる情報セキュリティ向上対策

パスワード設定・暗号化で盗難・紛失に備える

車上荒らしによるパソコンの盗難や、USBメモリの紛失。成績や住所録などの個人情報などが
入っていても、パスワードの設定やデータの暗号化をしておけば、盗み見や、流出したりする可
能性を低くすることが出来ます。

- 校務用パソコンはもちろん、個人所有のパソコンにもパスワード設定を
- 個人情報・重要情報ファイルにも、パスワード設定を

※原則として、特別な事情があり、管理職の許可の無い限り、個人情報は持ち出せません。

ウイルス対策ソフトの導入と基本ソフトのアップデートを

- パソコンにウイルス対策ソフトを導入し、アップデートを頻繁に
- Windowsなどの基本ソフトのアップデートの定期的実行を

ファイル共有ソフト(Winnyなど)は利用しない

- パソコンに保存しているファイルが勝手にネットワーク上に流出する等、危険がいっぱい

ソフトウェア・著作物の不正コピーをしない

- 不正コピー・配付することは刑事罰・損害賠償請求の対象(ウイルス感染で意図しない場合も同様)

宮崎県教育委員会