

1人1台の情報端末環境での情報安全・情報モラル

校内の教職員間で確認しておきたいチェックリスト

以下の項目で実際にできているか、□に✓をつけてみよう。

- (1) 児童生徒や教職員の情報端末のアカウント (ID) およびパスワードを適切に管理しているか。
- (2) 児童生徒や教職員に対して、アカウント (ID) およびパスワードを漏洩・紛失しないように指導しているか。
- (3) 児童生徒や教職員の情報端末の利用で問題が生じた場合に、即座にアカウント停止等の措置を行うことが徹底されているか。
- (4) アカウント (ID) やパスワードの意味や注意点を、教職員・保護者・児童生徒にわかりやすく説明しているか。
- (5) 児童生徒や教職員が他の児童生徒や教職員になりすまして利用する可能性がないか、確認しているか。
※情報端末およびログインカードを貸与、不正使用、パスワード流出。
- (6) 情報端末の利用履歴を確認する方法を、教職員が理解しているか。
例) メールやチャット、動画配信サービス、ゲームサイト等の制限
- (7) 教職員が情報端末の利用履歴を定期的に確認しているか。
- (8) ネットワーク上での危険な行動、他人に迷惑をかける行動をしないよう、児童生徒に注意を促す指導の機会を設けているか。
- (9) ネット上での誹謗中傷は犯罪であることを理解させ、ネット上での人権侵害を行わないように指導の機会を設けているか。
- (10) 児童生徒や保護者に対して、情報端末の活用の決まりやルールを考えたり話し合ったりする場を設けているか。

1人1台の情報端末環境での情報安全・情報モラル

教育委員会で確認しておきたいチェックリスト

以下の項目で実際にできているか、□に✓をつけてみよう。

- (1) 児童生徒や教職員の情報端末のアカウント（ID）の命名規則を定め、適切にアカウントを発行しているか。
- (2) 児童生徒や教職員の情報端末のパスワードの設定規則を定め、適切にパスワードを発行しているか。
- (3) アカウント（ID）やパスワードの意味や注意点を、教職員・保護者・児童生徒にわかりやすく説明しているか。
- (4) 児童生徒や教職員が他の児童生徒や教職員になりすまして利用する可能性がないか、確認しているか。
※情報端末およびログインカードを貸与、不正使用、パスワード流出。
- (5) 児童生徒が安心・安全が確保できるように、機能制限やフィルタリングなどの手段を適切に講じているか。
- (6) 情報端末の利用履歴を確認する方法を、教職員や保護者に説明しているか。
例) メールやチャット、動画配信サービス、ゲームサイト等の制限
- (7) ネットワーク上での危険な行動、他人に迷惑をかける行動をしないよう、児童生徒に注意を促す指導の機会を設けているか。
- (8) 児童生徒の情報端末の適切な取扱いや情報モラル教育に関する研修を定期的実施しているか。
- (9) ネット上での誹謗中傷やいじめが起きていないか、教育委員会が定期的に情報を収集しているか。
- (10) 各学校の情報安全や情報モラルに関する教育の取組状況について、教育委員会が把握しているか。