オンライン安全性方針

日本人学校

承認済み	**運営委員会**	**日付** 2024 年 2 月
最終レビュー日	2024 年 2 月	
次回のレビュー期限	2025 年 2 月	

バージョン番号	変更者	修正内容	変更日
1.0	岡本和男	オンライン安全方針の作成	24/11/2023

内容

---

1. 目的

私たちの学校は次のことを目指している：

- 児童生徒、職員、ボランティア、SMC のオンライン上の安全を確保するための強固なプロセスを整備する。
- オンライン上の危害のリスクが他の児童生徒よりも高い可能性のある児童生徒のグループを特定し、支援する。
- モバイルやスマートテクノロジー（私たちは「携帯電話」と呼んでいます）を含むテクノロジーの使用において、学校コミュニティ全体を保護し、教育する力を与えるオンライン安全への効果的なアプローチを提供する。
- インシデントを特定し、介入し、必要に応じてエスカレーションするための明確なメカニズムを確立する。

リスクの 4 つの主要カテゴリー

オンライン・セーフティに対する私たちのアプローチは、以下のリスク・カテゴリーへの対応に基づいている：

- **コンテンツ** - ポルノ、フェイクニュース、人種差別、女性差別、自傷行為、自殺、反ユダヤ主義、過激化、過激主義など、違法、不適切、または有害なコンテンツにさらされること。
- **接触**-他のユーザーとの有害なオンライン交流にさらされること。例えば、子どもどうしの圧力、商業広告、性的、犯罪的、金銭的、その他の目的で子どもや若者を手なずけたり搾取したりする意図で子どもや若者を装った大人など。
- **行為** - 露骨な画像の作成、送受信（ヌードやセミヌード、ポルノの同意のある共有、同意のない共有など）、その他の露骨な画像の共有、オンラインいじめなど、危害を加える可能性を高める、または危害をもたらす個人的なオンライン上での行動。
- **商業**-オンラインギャンブル、不適切な広告、フィッシングや金融詐欺などのリスク

2.法律とガイダンス

この方針は、教育省(DfE)の法定保護ガイダンスである「教育における子どもの安全の確保(Keeping Children Safe in Education)」と、その学校向けアドバイスに基づいている：

- 学校でのオンライン安全教育
- いじめとネットいじめの防止と取り組み：校長と学校職員のためのアドバイス
- 捜索、選別、没収

また、過激化から子どもを守るための DfE のガイダンスにも言及している。

これは、1996 年教育法（改正後）、2006 年教育・検査法、2010 年平等法などの現行法を反映したものである。さらに、2011 年教育法では、教員が「正当な理由」があると判断した場合、必要に応じて児童生徒の電子機器内の不適切な画像やファイルを検索し、削除することで、ネットいじめに対処する権限が強化されたことを反映している。

この方針は、当財団の資金提供契約および定款、ならびに日本の文部科学省による道徳教育に関する指導要領に準拠している。

この方針は、ナショナル・カリキュラムのコンピューティング学習プログラムも考慮に入れている。

3.役割と責任

3.1 学校運営委員会（SMC）

SMC はこの方針を監視し、その実施について校長に責任を負わせる全体的な責任を負う。

SMC は、すべての職員に、児童保護および保護教育の一環としてオンライン安全教育を受けさせ、職員がフィルタリングと監視に関する期待、役割、責任を理解するようにする。

また、運営委員会は、すべての職員が、効果的に児童生徒を保護するための関連スキルと知識を継続的に提供されるように、必要に応じて、また少なくとも年 1 回、定期的にオンライン安全に関する最新情報（電子メール、電子ニュースレター、職員会議を通じて）を受け取るようにする。

SMC は、適切な職員との定期的な会議を調整し、オンラインの安全性、研修の必要性について話し合い、指定保護責任者（DSL）が提供するオンラインの安全性ログを監視する。

SMC は、ネット上での安全確保を含め、子どもたちが自分自身や他人の安全を守る方法を確実に教えるべきである。

SMC は、学校が適切なフィルタリングと監視システムを学校デバイスと学校ネットワークに導入し、その有効性を定期的に見直しすることを保証しなければならない。**理事会**は、DfE のフィルタリングとモニタリングの基準を見直し、学校がその基準を満たすために何が必要か、IT 職員やサービスプロバイダーと話し合う：

- フィルタリングおよび監視システムを管理するための役割と責任を特定し、割り当てる；
- フィルタリングおよび監視規定を少なくとも年 1 回見直す；
- 教育や学習に不当な影響を与えることなく、有害で不適切なコンテンツをブロックする；

- 保護ニーズを満たす効果的なモニタリング戦略を実施する。

オンラインの安全性を監督する SMC のメンバーは、岡田茂樹運営委員長である。

SMC の全メンバーは

- 本方針を読み、理解したことを確認する。
- 学校の ICT システムとインターネットの使用に関する規約に同意し、遵守すること（付録 3）
- セーフガードや関連する方針・手順に対する学校またはカレッジ全体のアプローチを考案し、実施する際に、オンライン上の安全が継続的かつ相互に関連したテーマであることを確認する。
- 必要に応じて、ネット上の安全を含む保護に関する教育が、弱い立場の子ども、虐待の被害者、特別な教育的ニーズや障害（SEND）を持つ一部の児童生徒のために適応されるようにする。これは、「一律の」アプローチがすべての状況においてすべての児童生徒に適切であるとは限らないことを認識することが重要であり、より個人的な、あるいは状況に応じたアプローチがより適切である場合が多いためである。

3.2 校長

校長は、職員が本方針を理解し、学校全体で一貫して実施されていることを確認する責任がある。

3.3 指定保護責任者

本校の保護責任者(DSL)および代理の詳細は、児童保護および保護方針、および関連する職務記述書に記載されている。

DSL は、特に学校内のオンライン安全について主導的な責任を負います：

- 職員が本方針を理解し、学校全体で一貫して実施されるよう、校長をサポートする。
- 校長および運営委員会と協力し、本方針を毎年見直し、手順と実施方法が定期的に更新され、見直されるようにする。
- 学校用デバイスと学校ネットワークで実施されているフィルタリングと監視のシステムとプロセスを率先して理解する。
- ICT マネージャーと協力し、適切なシステムとプロセスが導入されていることを確認する。
- 必要に応じて、校長、ICT 管理者、その他の職員と協力し、オンラインの安全に関する問題やインシデントに対処する。
- 本校の児童保護方針に従い、オンライン上の安全に関するすべての問題やインシデントを管理する。
- オンライン安全に関するインシデントが記録され（付録 5 を参照）、本方針に従って適切に対処されるようにする。
- ネットいじめがあった場合、学校の行動方針に沿って記録され、適切に対処されるようにする。
- オンライン安全に関する職員研修の更新と実施（付録 4 には、オンライン安全に関する研修のニーズに関する職員の自己監査が記載されている）。
- 必要に応じて、他の機関や外部サービスとの連携。
- 学校におけるオンラインの安全性について、定期的に校長および/または運営委員会に報告する。
- 子どもたちが直面するリスクを考慮し、それを反映したリスクアセスメントを毎年実施する。
- 効果的な保護に必要なスキルと知識を継続的に提供するため、全職員に対し、少なくとも年 1 回、オンラインの安全性を含む保護と児童保護の最新情報を定期的に提供する。

このリストはすべてを網羅することを意図したものではない。

3.4 研究部／学校事務局

研究部／学校事務局が責任を負う：

- 学校用デバイスや学校ネットワーク上のフィルタリングや監視システムなど、適切なレベルのセキュリティ保護手順を導入し、少なくとも年 1 回は有効性を評価するために見直し、更新する。
- 学校の ICT システムが安全で、ウイルスやマルウェアから保護されていること、またそのような安全機構が定期的に更新されていることを確認する。
- 毎月、学校の ICT システムのセキュリティチェックと監視を行う。
- 潜在的に危険なサイトへのアクセスをブロックし、可能であれば潜在的に危険なファイルのダウンロードを防止する。
- オンライン安全に関するインシデントが記録され（付録 5 を参照）、本方針に従って適切に対処されるようにする。
- ネットいじめがあった場合、学校の行動方針に沿って適切に対処されるようにする。

このリストはすべてを網羅することを意図したものではない。

3.5 すべての職員とボランティア

請負業者や代理店職員を含むすべての職員、およびボランティアは、以下の責任を負う：

- 本方針の理解の維持
- この方針を一貫して実施する
- 学校の ICT システムとインターネットの使用に関する規約（付録 3）に同意し、遵守すること、また児童生徒が学校の使用に関する規約（付録 1、2）に従うようにすること。
- DSL がフィルタリングとモニタリングのシステムとプロセスに責任を負っていること、また、これらのシステムやプロセスが機能しなかった場合、学校事務局を通じて IIJ に報告する方法を知っていること。
- 教育目的でフィルタリングや監視システムを回避する必要がある場合は、学校事務局を通じて IIJ に連絡し、正しい手続きを踏むこと。
- DSL と協力し、オンライン安全インシデントが記録され（付録 5 参照）、本方針に沿って適切に対処されるようにする。
- ネットいじめがあった場合、学校の行動方針に沿って適切に対処されるようにする。
- オンライン・オフラインを問わず、性的暴力および／またはハラスメントに関するすべての報告や懸念に適切に対応し、「ここで起こるかもしれない」という態度を維持する。

このリストはすべてを網羅することを意図したものではない。

3.6 保護者

保護者には以下のことが期待される：

- 本方針に関する懸念や質問がある場合は、職員または校長に通知すること。
- 子どもが学校の ICT システムとインターネットの使用に関する規約（付録 1 と 2）を読み、理解し、同意していることを確認すること。
- 保護者は、以下の組織やウェブサイトから、オンラインで子どもを安全に保つためのガイダンスをさらに求めることができる：
- 問題点とは？ - 英国セーファーインターネットセンター
- ホットな話題 - チャイルドネット・インターナショナル
- 保護者向けリソースシート - チャイルドネット・インターナショナル

3.7 来校者と地域社会の人々

学校の ICT システムやインターネットを利用する来校者や地域の人々には、関連する場合、この方針が周知され、それを読み、従うことが期待される。適切な場合には、許容される使用に関する条件（付録 3）に同意することが求められる。

4.児童生徒へのオンライン安全教育

文部科学省による日本のカリキュラムに基づき、児童生徒たちにネットの安全について教える。

- 人間関係教育と健康教育 道徳教育 総合学習 小学校での学級活動
- 人間関係・性教育・健康教育、技術・家庭科、中等教育における道徳教育
- 文部科学省のカリキュラム 初等教育：
  https://www.mext.go.jp/content/20230308-mxt_kyoiku02-100002607_001.pdf
  (83 ページから 87 ページ)
- 中等教育：
  https://www.mext.go.jp/component/a_menu/education/micro_detail/__icsFiles/afieldfile/2011/01/05/1234912_011_1.pdf
  (9 ページ)
  https://www.mext.go.jp/component/a_menu/education/micro_detail/__icsFiles/afieldfile/2019/03/18/1387018_011.pdf
  (99 ページ)
  https://www.mext.go.jp/component/a_menu/education/micro_detail/__icsFiles/afieldfile/2019/03/18/1387018_001.pdf
  (84～86 ページ)

小学生は次のことを学ぶ：

- テクノロジーを安全かつ丁重に使用し、個人情報を保護する。
- インターネットやその他のオンライン技術上のコンテンツや接触について懸念がある場合、どこに相談すればよいかを確認する。
- テクノロジーを安全に、敬意を持って、責任を持って使用する。
- 容認できる行動と容認できない行動を認識する。
- 内容や接触に関する懸念を報告するためのさまざまな方法を特定する。

小学校を卒業するまでに、児童たちは次のことを学ぶ：

- ネット上では、自分を偽ることを含めて、人は時として異なる行動をとることがある。
- オンライン上の人間関係には、匿名である場合も含め、相手を尊重することの重要性を含め、対面での人間関係と同じ原則が適用されること。
- オンラインで安全に過ごすためのルールと原則、リスク、有害なコンテンツ、接触を認識する方法、およびそれらを報告する方法。
- ネット上の交友関係や情報源を批判的に検討する方法（会ったこともない人との交友に伴うリスクへの認識も含む）。
- 情報やデータがオンラインでどのように共有され、利用されるか。
- 仲間や他者との交友関係において、どのような境界線が適切か（デジタルの文脈も含む）。
- （オンラインを含むあらゆる状況において）見知らぬ大人に遭遇した場合、安全かつ適切に対応する方法。

KS3 では、児童生徒は次のことを学ぶ：

- オンライン上のアイデンティティとプライバシーの保護を含め、テクノロジーを安全、尊重、責任を持って安全に使用するためのさまざまな方法を理解する。
- 不適切な内容、接触、行為を認識し、懸念事項を報告する方法を知る。

中学生に教える：

- オンライン上のプライバシーやアイデンティティを保護する新しい方法など、テクノロジーの変化が安全にどのような影響を与えるかを理解する。
- さまざまな懸念事項の報告方法。

中等教育終了時までに、生徒たちは次のことがわかるようになる：

- オンラインを含むすべての状況において、同じ行動規範が適用されることを含む、オンラインでの権利、責任、機会。
- 誰かが他の人に提供した資料がオンラインで共有される可能性があること、オンラインに置かれた潜在的に危険な資料を削除するのが困難であることなど、オンライン上のリスクについて。
- 本人がそれ以上共有されることを望まない資料を他者に提供しないこと、および本人に送られた個人資料を共有しないこと。
- オンラインで資料を報告したり、問題を管理したりするために何をすべきか、どこでサポートを受けられるか。
- 有害コンテンツ視聴の影響。
- 特に性的に露骨なもの（ポルノなど）は、性行為の歪んだイメージを提示し、他者との関係において自分自身を見る目を傷つけ、性的パートナーに対する振る舞いに悪影響を及ぼす可能性があること。
- 児童のわいせつ画像（児童が作成したものを含む）の共有および閲覧は、懲役刑を含む厳罰を科す犯罪行為であること。
- 情報やデータがどのようにオンラインで生成、収集、共有、使用されるか。
- ネット上での有害な行為（いじめ、虐待、ハラスメントを含む）の見分け方と、そのような行為の被害を受けた場合の報告方法やサポートの探し方。
- 性的同意を含め、他者からの同意をどのように積極的に伝え、認識するか、また、いつ、どのように同意を撤回するか（オンラインを含むあらゆる状況において）。

ソーシャルメディアやインターネットの安全な使用については、関連する他の科目でも取り上げる。
必要であれば、ネット上の安全を含む保護に関する指導は、弱い立場の児童生徒、虐待の被害者、SEND を持つ一部の児童生徒に適応される。

5.保護者へのオンライン安全教育

本校は、手紙やその他の通信手段、本校のウェブサイトや仮想学習環境（VLE）を通じた情報により、保護者のインターネットの安全に対する意識を高める。この方針は保護者とも共有される。

授業参観日（保護者来校日）では、オンラインの安全についても取り上げる。

学校は保護者に知らせる：

- オンライン利用のフィルタリングと監視のために学校が使用しているシステム。
- 子どもたちがオンラインで何をするよう求められているか、アクセスするよう求められるサイトや、子どもたちがオンラインで交流する学校の関係者（もしいるのであれば）など。

保護者がオンラインの安全に関して質問や懸念がある場合は、まず、校長および/または DSL に知らせる。

本方針に関する懸念や質問は、職員または校長まで知らせる。

6.ネットいじめ

6.1 定義

ネットいじめは、SNS、メッセージングアプリ、ゲームサイトなど、オンライン上で行われる。他の形態のいじめと同様に、力の不均衡を伴う関係において、ある個人または集団が他の個人または集団に繰り返し意図的に危害を加えることである。(学校の行動方針も参照。）

6.2 いじめの防止と対策

ネットいじめを防止するため、児童生徒がネットいじめとは何か、また自分や他人がネットいじめに気づいたらどうすればよいかを理解できるようにする。被害者ではなく目撃者である場合も含め、児童生徒がどのように報告すればよいかを知り、報告するよう促す。

学校は、児童生徒といじめについて積極的に話し合い、いじめが起こる理由、いじめの形態、いじめの結果について説明する。学級担任は、受け持ち児童生徒といじめについて話し合う。

また、教職員は、カリキュラムの中でいじめを取り上げる機会を見つけるよう奨励されている。これには、PSHE（personal, social, health and economic）教育や、適切な場合には他の教科も含まれる。

全職員、運営委員、ボランティア（適切な場合）は、セーフガード研修の一環として、ネットいじめ、その影響、児童生徒をサポートする方法についての研修を受ける（詳細はセクション 11 を参照）。

学校はまた、保護者にネットいじめに関する情報やリーフレットを送り、いじめの兆候や報告方法、被害を受けた可能性のある子どもたちをどのようにサポートすればよいかを知らせている。
ネットいじめの具体的な事件に関しては、学校は学校の行動方針に定められたプロセスに従う。違法、不適切、または有害なものが児童生徒の間で広まっている場合、学校はその事件が収束するようあらゆる合理的な努力を払う。

DSL は、その資料の所持が違法であると疑うに足る合理的な根拠がある場合、合理的に実行可能な限り速やかに警察に事件を報告し、関連資料を提供する。また、必要と判断された場合は、外部のサービスとも連携する。

6.3 電子機器の検査

校長および校長から権限を与えられた職員は、捜索を実施し、疑わしい合理的な理由がある電子機器を没収することができる：

- 職員または児童生徒に危険を及ぼす、および/または
- 校則に、捜索を行うことができる禁止品目として明記されている、および/または
- 犯罪に関連する証拠
- 捜索の前に、権限を与えられた職員が、上記のいずれかを疑う合理的な理由があると納得した場合、職員はまた、捜索を行う：
- 捜索の緊急度を判断し、他の児童生徒や職員へのリスクを考慮する。捜索の緊急性が低い場合は、校長／DSL に助言を求める。
- なぜ検査を受けるのか、どのように検査が行われるのかを児童生徒に説明し、それについて質問する機会を与える。
- 児童生徒の協力を求める
-

権限を与えられた職員は、「正当な理由」があると判断した場合、押収した電子デバイス上のデータまたはファイルを調査し、例外的な状況においては消去することができる。

電子デバイス上のデータまたはファイルを調査する「正当な理由」があるかどうかを判断する際、職員は、そのデバイスが以下の目的で使用されている、または使用される可能性があると合理的に疑うべきである：

- 危害を加える、および/または
- 学校の安全な環境を損なう、または授業を妨害する。
- 犯罪を犯す

デバイスに不適切な資料が見つかった場合、適切な対応を決定するのは、校長と連携した DSL に任される。デバイス上に、人を危険にさらす可能性があると合理的に疑われる画像、データ、ファイルがある場合、まず適切な保護対応を検討する。

デバイスからデータまたはファイルを消去する正当な理由があるかどうかを判断する際、職員は、その資料が犯罪の容疑に関連する証拠となる可能性があるかどうかを考慮する。このような場合、職員は資料を削除せず、合理的に実行可能な限り速やかにデバイスを警察に渡す。その資料が犯罪に関連する証拠である疑いがない場合、職員は以下の場合にその資料を削除することができる：

- その存在が継続することにより、人に危害を及ぼす可能性があると合理的に疑われる場合、および/または
- 児童生徒および／または保護者が、自ら削除することを拒否した場合
- 児童生徒のわいせつな画像（ヌードまたはセミヌード画像とも呼ばれる）が機器に含まれている**可能性があると**職員が**疑った場合、**職員はその機器を使用する：
- 画像を表示**しない**
- デバイスを没収し、直ちに DSL（またはそれに相当する者）に報告する。DSL は、スクリーニング、検索、没収に関する DfE の最新ガイダンス、および UKCIS（UK Council for Internet Safety）の「ヌードおよびセミヌードの共有に関するガイダンス：児童生徒および青少年を対象とする教育現場への助言」に沿って決定を下す。

児童生徒の身体検査は、これに従って行われる：

- 捜索、審査、没収に関する DfE の最新ガイダンス
- ヌードおよびセミヌードの共有に関する UKCIS ガイダンス：児童生徒および青少年と関わる教育現場への助言
- 行動方針／いじめ防止方針

児童生徒の電子機器にある不適切な画像やファイルの検索や削除に関する苦情は、学校の苦情処理手続きを通じて処理される。

6.4 人工知能（AI）

ジェネレーティブ人工知能（AI）ツールは今や広く普及しており、簡単に利用できる。職員、児童生徒、保護者は、ChatGPT や Google Bard のような生成チャットボットに慣れているかもしれない。

ロンドン日本人学校は、AI は児童生徒の学習に役立つ多くの用途があるが、他者をいじめるために使われる可能性もあると認識している。例えば、AI を使って本物そっくりの画像や音声、動画を作り出す「ディープフェイク」だ。

ロンドン日本人学校は、AI を利用した児童生徒へのいじめを、いじめ防止／行動規範に則って取り扱う。

職員は、AI ツールがまだ開発されていない段階で AI ツールを使用することのリスクを認識し、学校で新しい AI ツールを使用する場合にはリスクアセスメントを実施すべきである。

7.学校でのインターネットの利用

すべての児童生徒、保護者、職員、ボランティア、運営委員は、学校の ICT システムとインターネットの使用に関する同意書に署名することが期待されている（付録 1〜3）。来校者は、本校の利用規約を読み、同意するものとする。

本校のインターネットの使用は、教育目的、または個人の職務を遂行する目的のみとする。

本校は、児童生徒、職員、ボランティア、運営委員、来校者（関連する場合）が閲覧するウェブサイトが上記を遵守していることを監視し、必要に応じてフィルタリングシステムによりアクセスを制限する。

詳細については、付録 1〜3 の使用承諾書に記載されている。

8.学校で携帯端末を使用する児童生徒

携帯端末を学校に持ち込むことは可能だが、学校内での使用は禁止されている。

児童生徒が学校内で携帯端末を使用する場合は、使用に関する同意書（付録 1 および 2 を参照）に従わなければならない。

児童生徒が利用規約に違反した場合、学校の行動方針に従って懲戒処分を受けることがある。

9.学校外での業務用機器の使用

全職員は、デバイスの安全性を確保するために適切な措置を講じる。これには以下が含まれるが、これらに限定されるものではない：

- デバイスをパスワードで保護する - 強力なパスワードは、大文字と小文字、数字、特殊文字（アスタリスクや通貨記号など）を組み合わせた、少なくとも 8 文字。
- ハードドライブが暗号化されていることを確認する - これは、デバイスが紛失または盗難にあった場合、新しいデバイスに取り付けることによって、誰もハードドライブに保存されたファイルにアクセスできないことを意味する。
- 一定時間非アクティブのままにしておくと、デバイスがロックされることを確認する。
- 家族や友人とデバイスを共有しない。
- アンチウイルスおよびアンチスパイウェアソフトウェアのインストール。
- 常に最新のアップデートをインストールし、オペレーティング・システムを最新の状態に保つ。

職員は、付録 3 に記載されている本校の利用規約に違反するような方法でデバイスを使用してはならない。

作業器具は、作業活動のみに使用しなければならない。

職員が自分のデバイスのセキュリティーに関して懸念がある場合は、研究部／事務局に助言を求めなければならない。

10.不正使用の問題に対する学校の対応

児童生徒が学校の ICT システムやインターネットを悪用した場合、本校は「行動」、「ICT」、「インターネットの使用」に関する方針に定められた手順に従う。取られる措置は、個々の状況、性質、具体的な事件の深刻さによって異なり、相応のものとなる。

職員が本校の ICT システムやインターネットを不正に使用した場合、または個人所有のデバイスを不正に使用した場合、その行為が不正行為に該当する場合、その問題は職員懲戒手続き/職員行動規範に従って処理される。取られる措置は、個々の状況、性質、具体的な事件の深刻さによって異なる。

学校は、違法行為や内容に関わる事件、またはその他の重大な事件を警察に報告すべきかどうかを検討する。

11.研修

すべての新入職員は、入社時研修の一環として、ネットいじめやネット上の過激化の危険性など、インターネットの安全な使用とネット上の保護問題について研修を受ける。

全職員は、保護教育の一環として、少なくとも毎年 1 回、再教育を受ける。

この研修によって、すべての職員は以下のことを認識することになる：

- テクノロジーは、多くの保護と福利の問題において重要な要素であり、子どもたちはオンライン虐待の危険にさらされている。
- 子どもたちはネット上で仲間を虐待することができる：
    - 虐待、嫌がらせ、女性差別的なメッセージ
    - わいせつなヌードやセミヌードの画像や動画を、特にチャットグループ内で無許可で共有すること。
    - 虐待画像やポルノを、そのようなコンテンツを受け取りたくない人たちと共有する。
- 身体的虐待、性的暴力、イニシエーション/ヘイジング型暴力はすべて、オンライン上の要素を含む可能性がある。

研修も職員の助けになる：

- オンライン虐待の兆候や症状を発見するための、より良い認識を養う。
- 児童生徒がオンライン活動における危険やリスクを認識し、リスクを考慮できるようにする能力を育成する。
- 児童生徒が長期的に最も健康的な選択をするよう影響を与え、短期的には危害から児童生徒を守る能力を養う。

DSL と DDSL は、少なくとも 2 年に 1 度、児童の保護と保護に関する研修を受ける。また、定期的に、少なくとも毎年、オンライン安全に関する知識とスキルを更新する。

運営委員は、セーフガード研修の一環として、安全なインターネットの使用とオンラインのセーフガード問題に関する研修を受ける。

ボランティアは適切な研修を受け、必要に応じて更新される。

保護研修の詳細については、児童保護および保護方針を参照のこと。

12.モニタリング

DSL は、オンラインの安全に関する行動と保護上の問題を記録する。インシデントレポートログは付録 5 にある。

この方針は、校長により毎年見直される。見直しのたびに、この方針は運営委員会と共有される。この見直しは、児童生徒がオン

ラインで直面するリスクを考慮し、反映させた年 1 回のリスクアセスメントによってサポートされる。テクノロジーやそれに関連するリスクや害は急速に進化し変化するため、これは重要なことである。

13.他の方針とのリンク

このオンライン安全方針は、本校の以下の方針とリンクしている：

- 児童保護と保護方針
- 行動方針
- 教職員の懲戒手続きに関する方針
- 苦情に関する方針と手続き
- いじめ防止方針
- 携帯電話方針

付録 1：初等教育での使用に関する同意書（児童生徒と保護者）

学校の ICT システムとインターネットの利用：児童生徒と保護者の同意書	
児童生徒の名前	
学校の ICT システム（コンピューターなど）を使い、学校でインターネットに接続するときは： • 使用する前に、先生や大人に使用できるかどうか尋ねる。 • 先生や大人に言われた、または許可されたウェブサイトのみを利用する。 • 次の場合はすぐに先生に伝えてください： 　o 間違ってウェブサイトを選択してしまった 　o 知らない人からメッセージを受け取る 　o 私や友人を動揺させたり傷つけたりする可能性のあるものを見つける • 学校のコンピュータは学業にのみ使用する • 他人に親切にし、動揺させたり失礼な態度をとったりしない。 • 学校の ICT 機器に気を配り、壊れたり、正常に動作しなかったりした場合はすぐに教員に伝える。 • 与えられたユーザー名とパスワードのみを使用する。 • ユーザー名とパスワードを一生懸命覚えようとする。 • 友人も含め、誰にもパスワードを教えない。 • 個人情報（氏名、住所、電話番号）を先生や保護者の許可なく他人に教えない。 • 学校のネットワークに自分の仕事を保存する。 • 印刷する前に先生に確認する。 • コンピュータを使い終わったら、ログオフするかシャットダウンする。 **私は、私が閲覧するウェブサイトを学校が監視すること、および私がルールに従わない場合は結果が生じることに同意します。**	
サイン（児童生徒）：	**日付**
保護者の同意　私は、学校の職員が適切に監督している場合、私の子どもが学校の ICT システムとインターネットを使用できることに同意します。私は、児童生徒が学校の ICT システムとインターネットを使用する際の上記の条件に同意し、子どもに理解させます。	
署名（保護者）：	**日付**

付録 2：中等教育での使用に関する同意書（児童生徒と保護者）

学校の ICT システムとインターネットの利用：児童生徒と保護者の同意書	
児童生徒の名前	
私は、利用規約の規則を読み、それに従います。 **学校の ICT システム（コンピューターなど）を使い、学校でインターネットに接続するときは：** • 学校の ICT システムとインターネットは、常に責任を持って教育目的のみに使用する。 • 先生が同席しているとき、または先生の許可があるときのみ使用する。 • 自分のユーザー名とパスワードを安全に保管し、他人と共有しない。 • 自分の個人情報を常に安全に保ち、先生や保護者の許可なく、私の名前、住所、電話番号を誰にも教えないこと。 • 自分や他人を動揺させたり、苦しめたり、危害を加えたりする可能性のある資料を見つけた場合は、すぐに先生（または良識ある大人）に伝える。 • 作業を終えたコンピューターは必ずログオフするかシャットダウンする。 **私がしないこと：** • 先生が学習活動の一環として明示的に許可した場合を除き、ソーシャルネットワーキングサイト、チャットルーム、ゲームサイトなど、不適切なウェブサイトにアクセスすること。 • 先生に確認せずにメールの添付ファイルを開いたり、メールのリンクをたどったりすること。 • 電子メールを含むオンラインでのコミュニケーションにおいて、不適切な言葉を使用する。 • ポルノ、攻撃的、わいせつ、またはその他の不適切な素材を作成、リンク、または投稿すること。 • 他人の情報を使って学校のネットワークにログインする。 • 親や保護者に相談することなく、または大人の監督なしに、オフラインで誰かと会う約束をする。 **私物の携帯電話やその他の電子機器を学校に持ち込む場合：** • 授業中、学級での時間、部活動、その他学校が主催する活動中、先生の許可なく使用しない。 • 私は責任を持って利用し、不適切なウェブサイトやその他の不適切な素材にアクセスしたり、オンラインコミュニケーションの際に不適切な言葉を使用したりしません。 **私は、私が閲覧するウェブサイトを学校が監視すること、および私がルールに従わない場合は結果が生じることに同意します。**	
サイン（児童生徒）：	**日付**
保護者の同意　私は、学校職員の適切な監督下で、私の子どもが学校の ICT システムとインターネットを使用することに同意します。私は、児童生徒が学校の ICT システムとインターネットを使用すること、および学校内で個人所有の電子機器を使用することに関する上記の条件に同意し、子どもにこれらを理解させます。	

学校の ICT システムとインターネットの利用：児童生徒と保護者の同意書	
署名（保護者）：	**日付**

付録 3：受諾可能な使用に関する同意書（教職員、運営委員、ボランティア、来校者）

学校の ICT システムとインターネットの利用：教職員、SMC、ボランティア、来校者のための同意書	
職員/運営委員/ボランティア/来校者の氏名：	
学校の ICT システムを使用し、学校内または学校外で業務用デバイス（該当する場合）でインターネットにアクセスする際、私は以下のことを行いません： • 暴力的、犯罪的、またはポルノ的性質を含む（ただし必ずしもこれらに限定されない）不適切な素材へのアクセス、またはアクセスを試みること（またはそのような素材を作成、共有、リンク、送信すること）。 • 学校の評判を損なうような方法で使用すること。 • ソーシャル・ネットワーキング・サイトやチャット・ルームへのアクセス • 電子メールやその他のメッセージングサービスを含め、オンライン上でコミュニケーションする際に不適切な言葉を使用すること。 • 許可されていないソフトウェアをインストールしたり、許可されていないハードウェアやデバイスを学校のネットワークに接続したりすること。 • パスワードを他人と共有したり、他人の情報を使って学校のネットワークにログインすること。 • 教員に確認せずに児童生徒の写真を撮ること。 • 学校、その児童生徒や職員、または他のコミュニティのメンバーに関する機密情報を共有する。 • データへのアクセス、修正、共有 アクセス、修正、共有の権限がない。 • 学校と直接関係のある事業でない限り、私企業を宣伝すること。	
私は、学校の ICT システムを使用し、学校内または学校外で業務用デバイスを使用してインターネットにアクセスするのは、教育目的または職務を遂行する目的に限ります。 私は、私が閲覧するウェブサイト、および学校の ICT 設備とシステムの使用を学校が監視することに同意します。 私は、仕事用のデバイスを学校外で使用する際は、安全でパスワードで保護されていることを確認し、本方針および学校のデータ保護方針に従ってすべてのデータを安全に保管するために、あらゆる合理的な手段を講じます。 私は、児童生徒から、彼らや他人を動揺させたり、苦しめたり、危害を加える可能性のある資料を見つけたと連絡があった場合、指定保護責任者（DSL）と ICT マネージャーに知らせます。 私は、学校の ICT システムとインターネットを常に責任を持って使用し、私の世話をする児童生徒にもそうさせます。	
署名（教職員／運営委員／ボランティア／来校者）：	**日付**

付録 4：オンライン安全研修の必要性 - 職員のための自己監査

オンライン安全研修・ニーズ監査	
職員／ボランティアの氏名	**日付**
質問	**はい/いいえ（必要に応じてコメントを追加）**
学校でのオンライン安全に関する責任者の名前を知っていますか？	
児童生徒がオンラインで仲間を虐待する可能性があることをご存知ですか？	
児童生徒から心配事や問題を持ちかけられたら、どうすべきか知っていますか？	
本校の職員、ボランティア、運営委員、来校者向けの利用規約をご存知ですか？	
児童生徒と保護者のための学校の利用規約をご存知ですか？	
学校のデバイスやネットワークのフィルタリングや監視システムに精通していますか？	
フィルタリングとモニタリングに関する自分の役割と責任を理解しているか？	
学校の ICT システムにアクセスするためのパスワードを定期的に変更していますか？	
ネットいじめに対する学校の取り組みをご存知ですか？	
オンライン・セーフティに関して、研修やさらなる研修を希望する分野はありますか？	

付録 5：オンライン安全インシデント報告ログ

オンライン安全インシデントログ				
日付	**事件が起きた場所**	**事件の概要**	**実施された措置**	**インシデントを記録した職員の氏名と署名**