
オンライン安全および適正利用方針 (AUP)

【改訂および用語】

本方針は、方針改定スケジュールに基づき定期的に見直しを行います。または法令等の変更があった場合に、必要に応じて改定します。

文書名	オンライン安全および適正利用方針
方針の区分	法令に関する方針
バージョン番号	2
作成者（役職）	Anthony Davies（事務局長）
承認者	学校長
認可者	ジェネラルマネージャー / 理事会
方針の発効日	2026 年 9 月 22 日
次回見直し予定日	2027 年 9 月 22 日

目次

1. 目的および適用範囲	3
2. 基本原則	3
3. 関連法令およびガイドライン	4
4. 役割および責任.....	5
5. 禁止事項・不適切な利用	7
6. 教職員（ガバナー、ボランティア、外部委託業者を含む）	10
7. Wi-Fi 経由のインターネット接続・アクセス	12
8. 学校ネットワークおよび ICT 設備の利用に関する監視・フィルタリング.....	13
9. 関連する他の方針・規程	14
10. 別紙様式 1：教職員向け 適性利用方針（AUP）同意書	15
11. 別紙様式 2：児童・生徒向け 適性利用方針（AUP）同意書	16

1. 目的および適用範囲

本オンライン安全および適正利用方針（AUP）は、校内におけるデジタル技術を安全に、責任を持って、かつ合法的に利用するための行動規範を定めるものです。本方針は以下の者に適用されます。

1.1 生徒・児童

1.2 教員およびサポートスタッフ

1.3 外部委託業者、来校者、ボランティア、および一時的な利用者

当校のオンライン安全への取り組みは、以下の4つのリスクカテゴリーに対処することに基づいています。

1.4 **コンテンツ**（情報内容）－違法、不適切または有害なコンテンツにさらされること。これには、ポルノグラフィ、フェイクニュース、人種差別、女性蔑視、自傷行為、自殺、反ユダヤ主義、過激化（ラディカリゼーション）および過激主義に関するコンテンツが含まれます。

1.5 **コンタクト**（連絡・接触）－他の利用者との有害なオンライン上のやり取りにさらされること。これには、同年代の者からの圧力（Peer-to-peer pressure）、商業広告、ならびに性的搾取、犯罪への勧誘、金銭的搾取、その他の目的で、大人が子どもや若者になりすまして接近する行為が含まれます。

1.6 **コンダクト**（オンライン上の行動）－危害につながる、または危害を受けるリスクを高める個人のオンライン上の行動。これには、性的に露骨な画像の作成、送信および受信（同意の有無を問わない裸体・半裸体画像の共有やポルノ画像の共有を含む。）、その他の不適切な画像の共有、ならびにオンラインいじめ（サイバーいじめ）が含まれます。

1.7 **コマー্স**（商業・金銭リスク）－オンラインギャンブル、不適切な広告、フィッシング詐欺、および／または金銭詐欺などのリスク。

2. 基本原則

当校は以下の事項に取り組むことを約束します。

2.1 児童・生徒、教職員、ボランティア、およびガバナーのオンライン上の安全を確保するため、強固な管理体制を整備します。

2.2 オンライン・セーフティに関する効果的な取り組みを実施し、携帯電話やスマートテクノロジー（以下、「携帯電話」という。）を含むテクノロジーの利用について、学校コミュニティ全体が安全に利用できるよう、適切な保護と教育を行います。

2.3 事案の早期発見、対応および必要に応じた報告・連携のための明確な体制と手順を確立します。

3. 関連法令およびガイドライン

3.1 本方針は、英国教育省（Department for Education：DfE）が定める法定児童生徒保護ガイドランス「Keeping Children Safe in Education（KCSiE）」ならびに学校向けに示されている以下の指針・助言に基づき策定されています。

- [Teaching online safety in schools](#)
- [Preventing and tackling bullying \(including cyber\)](#)
- [Relationships and sex education](#)
- [Searching, screening and confiscation](#)
- [Protecting learners from radicalisation](#)
- [National Cyber Security Centre \(NCSC\): Cyber Security for Schools](#)

3.2 本方針は、以下に掲げるものを含む既存の法令および関連法規を踏まえて策定されていますが、これらに限定されるものではありません。

- [The Computer Misuse Act 1990](#)
- [The Education Act 1996](#)
- [The Education and Inspections Act 2006](#)
- [The Equality Act 2010](#)
- [The Education Act 2011](#)
- [The Data Protection, Privacy and Electronic Communications \(Amendments etc\) \(EU Exit\) Regulations 2020](#) – UK GDPR
- [Education and Training \(Welfare of Children\) Act 2021](#)

3.3 15～18歳の生徒は、自然な好奇心を持っており、新しい考えや情報を探究することは、成長過程における自然な一部です。しかし、学校のシステムを利用する際には、適切な判断と責任ある行動が求められます。その際の基本的な指針として、「画面を同級生、教員、または保護者に見られても問題ないと思えるコンテンツのみを閲覧または検索する」という原則があります。もし他の人に見られないよう隠す必要があると感じるのであれば、そのコンテンツは学校のネットワークや端末で利用するには適切でない可能性があります。この基本的な指針は、教員、サポートスタッフおよび業務委託先のスタッフにも同様に適用されます。

3.4 学校の IT システムの利用者は、個人所有の電子機器や BYOD（Bring Your Own Device）端末など、学校の Wi-Fi ネットワークに接続されるすべての機器を含め、安全なオンラインアクセスを確保するための措置として、第三者によるアクセス制限、フィルタリングおよびモニタリングが行われることに同意するものとします。モニタリングは常時行われ

るものではなく、不適切なコンテンツへのアクセスまたは監視対象として設定されたキーワードが検知された場合にのみ作動します。

4. 役割および責任

4.1 理事会¹

理事会は、本方針の実施状況を監督するとともに、その実施について校長に責任を求める全般的な責任を負います。理事会は、以下を行います。

- 戦略的な監督を行う — 学校の理念、児童生徒の保護に関する取組、および長期的なデジタル戦略に沿った、包括的かつ最新の「適正利用規程（Acceptable Use Policy：AUP）」が学校に整備されていることを徹底する。
- 法令および規制への遵守を徹底する — AUP（適正利用方針）が、データ保護、児童生徒の保護（Safeguarding）、オンライン安全に関するガイダンス、および関連する学校評価・監査の枠組みを含む、法令上の義務を満たしていることを確認する。
- 説明責任と見直しを徹底する — 定期的な見直しを実施するとともに、法令・規程等の遵守状況および発生した事案について学校の管理職から報告を受け、AUPが効果的に実施されるよう、学校の管理職に対して説明責任を求める。

4.2 校長

校長は、責任を持って、教職員が本方針を理解し、学校全体で一貫してこれが実施されるように徹底します。

4.3 指定児童生徒保護責任者（Designated Safeguarding Leads：DSLs）

DSLは、学校におけるオンライン安全について主たる責任を担い、特に以下の事項を担当します。

- 教職員に本方針を周知徹底し、校内においてこれが一貫して実施されるよう管理する。
- IT担当の責任者、サービスプロバイダー、その他教職員と必要に応じて連携し、オンライン安全上の課題または問題に対処する。
- 学校の端末およびネットワークに導入されているフィルタリング並びに監視システム、およびその運用プロセスについて主導的に把握する。
- IT担当の責任者と連携し、適切なシステムおよびプロセスを確実に構築する。

¹ ジェネラルマネージャー、本部職員およびガバナーが一体となって実質的な理事会として機能し、最終的な意思決定権限は3名の主要ガバナーに帰属します。

- 学校の児童保護方針にのっとり、すべてのオンライン安全上の問題および事案を管理・対応する。
- オンライン安全上の問題が発生した際は、DSL がこれを確実に記録し、本方針に従って適切に処理する。
- サイバーいじめの事案が発生した際は、これを確実に記録し、学校の生徒指導方針にのっとり適切に処理する。
- オンライン安全に関する教職員研修を定期的に更新し、実施する。
- 必要に応じて、関係機関および外部サービスとの連絡調整を図る。
- 校内におけるオンライン安全の状況について、理事会に対し定期的に報告を行う。

4.4 本校の ICT サービスプロバイダー

本校の ICT サービスプロバイダーは、次の業務を行うものとします。

- 適切なレベルのセキュリティ対策を講じる。これには、フィルタリングおよびモニタリングシステム等の導入が含まれ、少なくとも年 1 回、IT 担当の責任者とともにその有効性を評価し、見直しおよび更新を行う。これにより、在校中の児童・生徒が、テロリストや過激主義に関するコンテンツを含む、オンライン上の潜在的に有害または不適切なコンテンツや接触から確実に保護されるようにする。
- 学校の ICT システムが安全に管理され、ウイルスやその他の悪意のあるソフトウェアから保護されていることを確認するとともに、これらのセキュリティ対策が定期的に更新されるようにする。
- 定期的な全面セキュリティチェックを実施し、学校の ICT システムを監視する。
- 危険性のあるウェブサイトへのアクセスをブロックし、可能な限り、危険性のあるファイルのダウンロードを防止する。

4.5 全教職員およびボランティア

すべての教職員（業務委託先のスタッフおよび派遣スタッフを含む）ならびにボランティアは、以下について責任を負います。

- 本方針を十分に理解し、これを遵守するとともに、他の関係者による本方針の適切な実施を確認する。
- 学校の ICT システムおよびインターネットの利用同意書（付録 1）に同意してこれを遵守するとともに、生徒が学校の利用同意書（付録 2）を確実に遵守するよう指導する。

- DSL と連携し、オンライン安全上の事案が学校によって確実に記録され、本方針に従って適切に処理されるようにする。
- フィルタリングおよび監視システム、並びにその運用プロセスについての責任は DSL が負っていることを認識し、当該システムまたはプロセスに不具合が生じた際の報告方法を熟知しておく。
- サイバーいじめの事案が発生した際は、学校の生徒指導方針に従い適切に対応されるようにする。
- オンラインおよびオフラインの双方における性暴力および性的ハラスメントに関するすべての報告や懸念に対し適切に対応し、「この学校でも起こり得る」という危機意識を常に保持する。

4.6 保護者および養育者

保護者および養育者は、次の事項を遵守していただきます。

- すべての児童・生徒にとって安全で、互いに尊重し合える安心なオンライン環境を維持するため、学校と連携して取り組むことに同意する。
- 学校のオンライン安全管理への取り組みを支持し、教職員から共有される指導指針に従うとともに、子どもが家庭および学校において責任を持ってテクノロジーを利用するよう促す。
- 問題が生じた場合には、速やかに対応し、建設的に解決できるよう、校長または指定児童生徒保護責任者（Designated Safeguarding Lead：DSL）に速やかに連絡する。
- 適性利用方針への違反が生じた場合は、子どもの最善の利益を第一に考え、問題の解決に向けて学校に全面的に協力する。

保護者は、インターネットの利用および子どものオンライン上の安全確保に関するアドバイスやガイダンスについて、The UK Safer Internet Centre、および Childnet から情報を得ることができます。

5. 禁止事項・不適切な利用

学校の ICT 設備を以下のように利用することは、不適切な利用とみなします。当方針へのいかなる違反も、懲戒手続または生徒指導上の処分の対象となる場合があります。（下記のセクション 5.3 を参照のこと）

学校の ICT 設備の不適切な利用には、以下にあげる行為が含まれます。

- 学校の ICT 設備を利用して、知的財産権または著作権を侵害すること。
- 学校の ICT 設備を利用して、他者をいじめ、若しくはハラスメントを行うこと、または不法な差別を助長すること。
- 学校の方針または手続に違反すること。
- あらゆる違法行為、または違法活動を推奨するとみなされる言動を行うこと。
- オンラインギャンブル、不適切な広告、フィッシング、および／または金融詐欺を行うこと。
- ポルノ、攻撃的、わいせつ、あるいはその他不適切もしくは有害なコンテンツにアクセス、作成、保存、リンク、または送信すること。
- 合意の有無を問わず、裸体および半裸体の画像、動画、および／またはライブストリームを共有すること。
- 学校を誹謗中傷もしくは軽視する活動、または学校の名誉を毀損する恐れのある活動を行うこと。
- 学校、生徒、または学校関係者に関する機密情報を共有すること。
- 権限のある担当者の承認を得ることなく、端末を学校の ICT ネットワークに接続すること。
- 権限のある担当者の承認を得ることなく、学校のネットワーク上にソフトウェア、アプリケーション、またはウェブサービスを設置すること。並びに、学校の ICT 設備、アカウント、またはデータの機能を妨害するように設計されたプログラム、ツール、若しくはソフトウェアを作成または利用すること。
- 権限のある担当者の承認を得ることなく、ネットワークの制限区域、またはパスワードで保護された情報にアクセス、若しくはアクセスを試みること。
- 他者が学校の ICT 設備に不正にアクセスすること（または不正アクセスを試みること）を許可、奨励、または可能にすること。
- 学校の ICT 設備に故意に損害を与えること。
- 権限のある担当者の承認を得ることなく、学校の ICT 機器、システム、プログラム、または情報を移動、削除、または処分すること。
- 権限のある担当者からアクセスを許可されていない、または権限のないデータ（個人データを含む）にアクセス、変更、もしくは共有することにより、データ侵害を引き起こすこと。

- 不適切または攻撃的な言葉を使用すること。
- 学校と直接関係のある事業を除き、私的な事業を宣伝または促進すること。
- 学校のフィルタリングまたは監視メカニズムを回避するためのウェブサイトや仕組みを利用すること。
- 過激化、過激主義、人種差別、反ユダヤ主義、またはその他いかなる形態の差別にも該当するコンテンツや行為に関与すること。
- 学校の IT 担当職員または適切な審査を完了した IT パートナー企業以外の者が、学校の IT ハードウェア、ソフトウェア、システムまたは IT インフラに対して、いかなる作業も行ってはならない。
- AI ツールおよび生成 AI チャットボット（ChatGPT など）を以下のように利用すること。
 - 内部評価・外部評価を含む評価および課題（コースワーク）の実施中に使用すること。
 - AI が生成した文章や画像を自分自身が作成した作品であるかのように使用して、宿題や授業の課題を作成すること。

以上はすべてを網羅した一覧ではありません。学校は、必要に応じていつでもこの一覧を変更する権利を有します。上記の一覧に記載されていない行為または行動についても、学校の IT 設備の不適切な利用に該当するかどうかは、校長がその専門的判断に基づいて決定します。

5.2 禁止行為の例外

学校の ICT 設備を校内または校外（リモート環境を含む）で利用する場合において、その利用目的が通常であれば本方針上の不適切な利用に該当すると考えられるものであっても、校長が必要と認めた場合には、その裁量により本方針の例外を認めることがあります。

生徒は、以下の場合に限り、AI ツールおよび生成 AI チャットボットを利用することができるものとします。

- 新しいトピックやアイデアについて調べるためのリサーチツールとして利用する場合。
- 授業や課題において AI そのものを学習・検討する場合（例：情報科の授業や、AI 生成画像を題材とした美術の課題など）。ただし、AI によって生成されたすべてのコンテンツについては、その旨を適切に明示し、出典を明確にしなければならない。

5.3 懲戒措置

上記に掲げる不適切な行為を行った生徒または教職員は、学校の行動規範（Behaviour Policy）または教職員行動規範（Staff Code of Conduct）に基づき、懲戒その他の適切な措置の対象となる場合があります。

6. 教職員（ガバナー、ボランティア、および業務委託先スタッフを含む）

6.1 学校の ICT 設備および資料へのアクセス

学校のネットワーク管理者（Network Manager）は、教職員による学校の ICT 設備および情報資産へのアクセス管理を担当します。これには、以下を含みますが、これらに限定されるものではありません。

- コンピュータ、タブレット、携帯電話、およびその他の端末
- 特定のプログラムまたはファイルへのアクセス権限。

教職員には、学校の ICT 設備にアクセスする際に使用する固有のログイン／アカウント情報およびパスワードが与えられます。閲覧または編集の権限を付与されていないファイルへのアクセスが可能となっている場合、またはアクセス権限の変更・更新が必要な場合には、当該教職員は直属の上司（Line Manager）に速やかに報告するものとしします。

6.2 電話および電子メールの利用

学校は、各教職員に学校用の電子メールアドレスを付与します。この電子メールアカウントは業務目的にのみ使用するものとし、学校に関する業務上の連絡はすべて学校が提供する電子メールアドレスを用いて行わなければなりません。

教職員は、自身の個人用メールアドレスを保護者、養育者、または生徒に共有してはならず、個人用メールアドレスを使用して業務関連の資料を送信してはいけません。

教職員は、電子メールの内容に十分注意しなければなりません。不適切または不正確な記載は、差別、ハラスメント、名誉毀損、守秘義務違反または契約違反に関する申し立てや法的責任を招く可能性があります。

電子メールは、紙の文書と同様に、法的手続において開示が求められる場合があります。また、2018 年データ保護法（Data Protection Act 2018）に基づく個人からの請求に応じて、開示の対象となる場合があります。利用者の受信トレイから電子メールを削除したとしても、開示のためにその電子メールを復元できなくなるわけではありませ

ん。すべての電子メールは、開示のために復元される可能性があるものとして取り扱わなければなりません。

教職員は、機密情報または機密性の高い情報を電子メールで送信する際、特に細心の注意を払わなくてはなりません。機密情報または機密性の高い情報を含む添付ファイルは、意図した受信者のみがアクセスできるよう暗号化する必要があります。

教職員が誤って送信された電子メールを受信した場合は、送信者にその旨を通知し、当該電子メールを削除しなければなりません。電子メールに機密性の高い情報または秘密情報が含まれている場合、受信者はその情報を利用したり、第三者に開示したりしてはなりません。

教職員が、他人の個人情報を含む電子メールを誤って送信した場合は、直ちに事務長（Bursar）に報告し、学校のデータ漏洩対応手順に従わなくてはなりません。

教職員は、自身の個人用電話番号を保護者、養育者、または生徒に教えてはいけません。教職員は、すべての業務関連の用務を行うにあたり、学校が支給した電話を使用しなくてはなりません。

学校の電話を私用目的で使用してはなりません。職務上の備品として携帯電話を支給されている教職員は、セクション 5 に定める ICT 利用規約と同様の規則を遵守する必要があります。

6.3 私的利用

教職員は、以下に定める一定の条件に従うことを前提として、学校の ICT 設備を私的に利用することが認められます。ただし、当該許可を過度に使用したり、または乱用してはなりません。校長は、自らの裁量により、いつでも当該許可を取り消し、または制限することができます。

私的利用は、以下の条件を満たす場合に限り認められます。

- 授業や指導時間内に行わない。
- セクション 5 に定義される「不適切な利用」に該当しない。
- 生徒がその場にいないとき。
- 業務に支障をきたさず、また、他の教職員や児童・生徒が業務上または教育上の目的で学校の ICT 設備を利用することを妨げない。

教職員は、学校の ICT 設備に、業務に関連しない私的な情報または資料（音楽、動画、写真など）を保存してはなりません。

教職員は、学校の ICT 設備を私的に利用することにより、私的な通信内容が学校の ICT 監視活動の対象（セクション 8 を参照のこと）となる可能性があることを認識す

る必要があります。本方針への違反が判明した場合は、懲戒処分の対象となる場合があります。

教職員は、教職員行動規範に従い、自身の個人用端末（携帯電話やタブレットなど）を使用することも認められます。

教職員は、学校の ICT 設備を使用していない場合であっても、ICT の個人的な利用が雇用関係に影響を及ぼす可能性があることを認識しなければなりません。例えば、生徒や保護者が閲覧できる形で、個人情報をインターネット上に公開することなどが該当します。

教職員は、オンライン上で自身を適切に保護し、専門職としての信頼性や品位を損なうことのないよう、ソーシャルメディアおよび電子メールの利用に関する学校のガイドラインを遵守するよう十分注意しなければなりません。

6.4 リモートアクセス

学校は、教職員が遠隔地から学校の ICT 設備および資料にアクセスすることを許可します。遠隔アクセスは、学校支給のノート PC のみを使用し、暗号化された VPN を介して接続する必要があります。

教職員が学校の ICT 設備および情報資産にリモートでアクセスする場合は、校内でこれらの設備および情報資産を利用する場合と同じ規則を遵守しなければなりません。学校外で学校の ICT 設備を使用する場合、教職員は特に注意を払い、ウイルスの持ち込みやシステムのセキュリティを損なうことを防ぐため、ネットワーク管理者または校長がその都度求める必要な予防措置を講じなければなりません。

当校の ICT 設備には、機密情報、および／またはデータ保護法制の対象となる情報が含まれています。当該情報は、細心の注意を払い、かつ学校のデータ保護方針に従って取り扱わなければなりません。

学校のデータ保護方針は、学校のウェブサイトにおいて確認することができます。

7. Wi-Fi 経由のインターネット接続

学校の無線インターネット接続（Wi-Fi）は暗号化により保護されており、不適切なサイトへのアクセスを防止するためのフィルタリングが適用されています。学校は、用途に応じて複数の Wi-Fi（教職員用、生徒用、ゲスト用など）を設置しており、利用者は自身にアクセス権限が付与されている Wi-Fi にのみ接続するものとします。また、パスワードを他者と共有してはなりません。

インターネットへのアクセスにどの Wi-Fi を使用した場合であっても、学校の ICT 監視活動（セクション 8 を参照のこと）は継続して適用されるものとします。禁止される行為（セク

ション 5) に違反した者は、個人用端末からアクセスした場合であっても、処分に関して同様の扱いを受けるものとします。

8. 学校ネットワークおよび ICT 設備の利用に関する監視・フィルタリング

児童・生徒の福祉を保護・促進し、安全に学習できる環境を提供するため、学校は、その ICT 設備およびネットワークの利用をフィルタリングおよび監視する権利を留保します。これには、以下の事項のフィルタリングおよび監視が含まれますが、これらに限定されるものではありません。

- 閲覧したインターネットサイト
- 帯域幅（通信量）の使用状況
- 電子メールアカウント
- ユーザーのアクティビティ／アクセスログ
- その他一切の電子通信

権限を有する ICT 担当職員のみが、法令で認められる範囲内において、上記項目のフィルタリング、検査、監視、傍受、評価、記録、および開示を行うことができるものとします。

学校が ICT の利用状況を監視する目的は、以下になります。

- 学校業務に関連する情報を取得するため
- 学校の方針、手続きおよび基準への遵守状況を調査するため
- 学校運営および ICT システムの効果的な運用を確保するため
- 研修または品質管理のための取り組みを実施するため
- 犯罪を防止または発見するため
- 情報開示請求（Subject Access Request）、情報公開法（Freedom of Information Act）に基づく請求、またはその他の法的義務に対応するため
- 利用者の安全保護（Safeguarding）を確保するため

当校の理事会は、学校が英国教育省（DfE）のフィルタリングおよび監視に関するコア基準（filtering and monitoring core standards）を満たしていることを確保するとともに、以下の事項について責任を負います。

- 適切なフィルタリングおよび監視システムが導入されていること。

- 教職員がこれらのシステムについて理解しており、それぞれに関連する役割および責任について適切な研修を受けていること。
- 管理職チームおよび関係教職員に対しては、プロセスおよびシステムを効果的に管理する方法、並びに懸念事項をエスカレーション（上位報告）する方法が含まれていること。
- 学校の監視およびフィルタリングシステムの有効性を定期的に見直すこと。

学校の指定児童生徒保護責任者（DSL）は、本校で導入されているフィルタリングおよび監視システムならびに関連する運用手順について把握し、その適切な運用を主導する責任を負います。教職員は、必要に応じて、監視によって確認された ICT 利用上の懸念事項を、DSL または ICT 管理責任者に報告するものとします。

9. 関連する方針・規程

- 児童生徒保護（セーフガーディング）方針
- 生徒指導方針
- 教職員行動規範
- データ保護方針

様式 1：教職員向け 適性利用方針同意書 - ガバナー、ボランティアおよび来校者にも適用

学校の ICT 設備およびインターネットの適正利用に関する同意書 （教職員、学校理事、ボランティアおよび来校者対象）	
氏名：	
所属機関／団体名：	
学校の ICT 設備を利用する際、または学校内からインターネットにアクセスする際、あるいは学校外で業務用端末を使用してインターネットにアクセスする際、以下の行為を行わないことに同意します。 - 不適切なコンテンツにアクセスしたり、アクセスを試みる。これには、暴力的、犯罪的またはポルノグラフィーに関するコンテンツなどが含まれるが、これらに限定されない。また、そのようなコンテンツを作成、共有、リンク、送信する。 - ICT 設備やインターネットを利用して学校の評判や信用を損なう恐れのある行為を行う。 - 私の職務上の責任または学校の方針に反する形で、ソーシャルネットワーキングサイトやチャットルームにアクセスする。 - メールやその他のメッセージサービスを含め、オンライン上でのコミュニケーションにおいて、不適切な言葉を使う。 - 承認されていないソフトウェアのインストール、承認されていないハードウェアや端末を学校のネットワークに接続する。不明な点や判断に迷う点がある場合は、Aztech に相談します。 - 自分のパスワードを他者と共有したり、他者のログイン情報を使用して学校のネットワークにログインする。 - 学校、生徒、教職員、その他学校関係者に関する機密情報を共有する。 - 自分にアクセス、変更または共有する権限が与えられていないデータにアクセスしたり、変更したり、共有する。 - 学校と直接関係のある事業を除き、個人または私的な事業の宣伝をする。	
私は、学校が私の閲覧したウェブサイトおよび学校の ICT 設備・システムの利用状況を監視することを理解しています。 学校外で業務用端末を使用する際は、端末の安全を確保し、パスワードで保護するために合理的かつ必要な措置を講じます。また、本ポリシーおよび学校のデータ保護ポリシーに従い、すべてのデータを安全に保管します。 児童・生徒から、自分自身または他者を不安にさせたり、苦痛を与えたり、危害を及ぼす可能性のあるコンテンツを見つけたと報告を受けた場合、または私自身がそのようなコンテンツを発見した場合は、DSL および ICT 管理責任者に報告します。 私は、常に責任を持って学校の ICT システムおよびインターネットを利用し、担当する生徒に対しても同様に利用させます。	
署名：	日付：

様式 2：児童・生徒向け 適性利用方針同意書

学校の ICT 設備およびインターネットの適正利用に関する同意書 (児童・生徒対象)
氏名：
学校の ICT 設備を利用する際、および校内でインターネットにアクセスする際、以下の行為を行わないことに同意します。 ● 学校時間中に、教育目的以外で学校の ICT 設備やインターネットを利用する。 ● 学校時間中に、教員が同席していない、または教員の許可を得ることなく利用する。ただし、正式に認められた自主学習時間の一部として使用する場合を除く。 ● 学校の規則に違反する目的で利用する。 ● 不適切なウェブサイトアクセスする。 ● ソーシャルネットワーキングサイト（SNS）にアクセスする。ただし、学習活動の一環として教員が許可した場合を除く。 ● チャットルームを利用する。ただし、教員の監督の下で教育目的のために学校が承認したサービスを利用する場合を除く。 ● 事前に教員に確認することなく、電子メールの添付ファイルを開いたり、または電子メール内のリンクをクリックする。ただし、その電子メールまたはリンクが、教員や学校が承認した教育サービスなど、既知かつ信頼できる送信元からのものである場合を除く。 ● メールを含むオンライン上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。 ● 写真や動画に写っている人物の合意がある場合であっても、半裸体または裸体の画像、動画、ライブストリームを共有する。 ● 自分のパスワードを他者と共有したり、または他者のログイン情報を用いて学校のネットワークにログインしたりする。 ● 他者をいじめたり、嫌がらせをしたりする。 ● AI ツールおよび生成 AI チャットボット（ChatGPT など）を以下の目的で使用する。 - 内部評価・外部評価を含む試験・評価や課題、並びにコースワークにおいて使用する。 - AI が生成した文章や画像を、自分自身が作成した作品であるかのように提出・提示する。 ● 寮生は、学校の寮の規則、オンライン安全に関する規定、およびセーフガーディング上の理由により課される制限に従うことを条件として、学校時間外に保護者、後見人、家族および友人との連絡のためにソーシャルメディアやメッセージングサービスを利用することができる。 ● 学校時間外にソーシャルメディアを利用する際は、自分自身または他者を危険にさらす可能性のある個人情報を共有せず、オンライン上でのみ知り合った人物と会わない、また、サイバーいじめ、嫌がらせその他の不適切なオンライン行為を行わないこと。

私は、学校が私の閲覧したウェブサイトおよび学校の ICT 設備・システムの利用状況を監視することを理解しています。

自分自身または他者を不安にさせたり、苦痛を与えたり、危害を及ぼす可能性のあるコンテンツを見つけた場合は、直ちに教員またはその他の教職員に報告します。

私は、常に責任を持って学校の ICT システムおよびインターネットを利用します。

校外にいるときにオンライン上で行った行為であっても、学校が不適切な行為として定めている場合には、学校から指導や処分を受けることがあることを理解しています。

署名：

日付：