

メタバース空間を活用した不登校児童生徒支援業務委託仕様書

1 業務名

メタバース空間を活用した不登校児童生徒支援業務

2 目的

大分市の小中学校及び義務教育学校に在籍する児童生徒のうち、学校や相談機関等に通うことが難しい不登校状態の児童生徒に対して、メタバース空間における人とのつながりや心の居場所づくりなど、個々の実態に応じた支援の充実を図る

3 履行期間

契約締結日から令和8年3月31日まで

4 履行場所

大分市教育委員会 教育部 児童生徒支援課

5 利用対象

大分市の小中学校及び義務教育学校に在籍する児童生徒のうち不登校状態の児童生徒
20名程度（見込み）

6 業務委託内容

(1) 環境構築

① 基本仕様について

ア クラウド空間上でのサービスであり、各小中学校及び義務教育学校、家庭等から利用可能であること。

イ 利用中のデータ通信は、SSL/TLS等で暗号化され、第三者による盗み見等が防止されること。

ウ 専用ソフトウェアをインストールする必要がなく、「Safari」及び「Google Chrome」、「Microsoft Edge」等の標準的なブラウザで利用可能であること。

エ 機能アップデート、内容の修正等が行われた際には、追加費用なく適応されること。
また、その際にユーザー側の操作なく反映されること。

② メタバース空間について

ア プラットフォームは、日本国内の事業者が提供するものを使用すること。

イ 開室時間については、平日のうち週2回以上、かつ1日2時間以上を想定している。

ウ メタバース空間内は、複数のスペースを作成できること。

エ スペースにおいてカウンセリング等を行うことができるよう申込みの受付やオンラインでの個別面談が可能であること。

オ 同時接続可能アカウント数は最低10アカウントとすること。

③ アバターについて

- ア 用意された中から、利用者が自由に選択できこと。
- イ プロフィール等利用者が自由に変更できること。
- ウ ネームプレート等による表示ができること。

④ 利用者機能について

- ア アバターを自由に動かせ、音声やテキスト等による他者との交流や空間内の活動がスムーズに行えること。
- イ 利用者用として最低20アカウント以上を提供可能であること。
- ウ 利用者がメタバースにログインしたり、他者とのコミュニケーションをとったりするための意欲向上等を目的とした機能が備え付けられていれば提案すること。

⑤ 管理者機能について

- ア 特定またはすべての利用者に対してメッセージが届けられること。
- イ 他者を攻撃したり活動を妨害したりするなど、不適切な行為をしたユーザーを利用停止させるなどの秩序維持のための措置を実施できること。また、利用停止等の措置を解除できること。
- ウ 利用者について、ログイン、ログアウト状況のデータが取得できること。また、管理者側で、利用者のビデオ通話（誰と誰がいつどれだけ通話したか）やチャット（チャットの内容）の使用状況等について把握できる機能があれば提案すること。
- エ 利用者がログインできる時間帯を設定でき、時間終了により、自動で利用者を強制的に一斉ログアウトさせることができること。
- オ 管理者側で、利用者がメタバース空間にログインする際のパスワードを設定できること。また、パスワードの設定又は解除が切り替えられること。
- カ 管理者用として最低5アカウント以上を提供可能であること。

(2) 管理者及び利用者向けのマニュアル作成

管理者及び利用者が、機能や操作についてスムーズに理解できるようなマニュアルを作成すること。

(3) サポート及び研修

サポート窓口の設置、操作動画や研修資料を提供すること。その他、サポートや研修についての具体的な取組があれば提案すること。

(4) セキュリティ対策

- ① メタバース空間の利用に係るセキュリティ及び個人情報保護の取り扱いについては、個人情報の保護に関する法律等の関連法規を遵守することはもちろんのこと、本市条例及び規則等を遵守し、適切に実施すること。また、契約に定める目的以外でのデータ利用は行わないこと。さらに、本業務に関して知り得た情報の漏洩、滅失、き損の防止、その他の適正な管理のため必要な措置を講じなければならない、契約終了後も同様とする。

- ② データの保存先（データセンター等）は、データ損失対策、情報漏洩対策がなされていること。また、データ管理を行う企業においては、「プライバシーマーク」等の情報セキュリティやクラウドサービスセキュリティ等に関する第三者認証を得ていること。
- ③ 情報セキュリティ事故が発生した場合は、速やかに事故の原因を特定するとともに、その内容及び対応について担当課（児童生徒支援課）宛てに報告を行うこと。
- ④ システムのデータについては、障害発生時に備えて、バックアップ、予備装置を配置するなど、適切に保護されていること。

6 追加提案

本仕様書に定めるもののほか、追加提案があれば提案書に含めること。

追加提案の例：利用者が継続して利用し続けることができるようにするためのサポート、メタバース空間における活動案の提供、他市等の活用状況の情報提供、利用者の興味が湧くような動画等の情報提供、コミュニケーション時の不適切な投稿、発言等の管理機能等

7 機密保持等

受託者は、本契約における機密情報の取扱いについて、次の事項を遵守しなければならない。

- (1) 作業上知り得た委託者の機密情報について、第三者に漏洩してはならない。
- (2) 委託者が作業上必要と認めて貸与するデータの内部情報については、散逸、漏洩、目的外使用等の事故が起きないように十分注意し、取扱うこと。
- (3) 全てのデータの取扱いについて「個人情報保護法」及び別紙1「大分市立学校における情報セキュリティの基本方針」を遵守すること。
- (4) 故意、過失を問わずデータ流出事故が発生した場合は、委託者が指示する手続きに従い、速やかに報告を行うこと。また、事故により損害を与えた場合は、その損害を補償すること。
- (5) 受託者は、個人情報等の本業務作業に関して知り得た一切の事項を、契約期間のみならず、終了後も第三者へ漏洩してはならない。
- (6) 受託者は、委託者が文書により承認したとき以外は、本業務に係る一切の資料及び記録媒体（以下「資料等」という。）を本業務以外の用途に使用してはならない。また、本業務に係る資料等を第三者に提供、又は譲渡してはならない。
- (7) 受託者は、委託者が許可した場合を除き、資料等を複写又は複製してはならない。委託者の許可を得て複写又は複製したときは、本業務の終了後、直ちに複写又は複製した資料等を消去し、再生及び再利用ができない状態にしなければならない。
- (8) 受託者が、本業務で作成された資料等が第三者の知的財産権を侵害していないことを保証すること。また、本業務で作成された資料等の著作権は、委託者に帰属するものとする。ただし、特段の事情があり、発注者が認めた場合はこの限りではない。
- (9) 受託者は、機密情報を記した書面その他物件は、施錠できる場所に保管し、厳重に機密を保持しなければならない。

- (10) 受託者は、資料等について、本業務終了後に委託者へ返還しなければならない。また、委託者及び受託者は、本業務に係る個人情報の授受に従事する者を指定し、当該個人情報の授受に際しては預かり証を提出しなければならない。受託者は、本業務に係る個人情報を暗号化して、施錠できるケースに収納し、事故防止措置を講じた上で搬送しなければならない。
- (11) 受託者は、個人情報の漏洩を防止するため、本業務を第三者に委託してはならない。ただし、本業務の一部についてやむを得ず第三者に委託する必要がある場合は、あらかじめ再委託する業者名、作業内容、作業場所等を委託者に届け出て、委託者の承認を得なければならない。また、再委託を受けた者に対しても、機密保持等について同様の義務を負わせなければならない。
- (12) 受託者は、以上の事項に違反して委託者又は第三者に損害を与えたときは、その損害を賠償しなければならない。委託者が受託者の違反行為につき、第三者から損害の賠償を求められたときも同様とする。

8 その他

- (1) この仕様書に定めのない事項又は疑義が生じた場合は、必要に応じて本市と協議の上、誠意をもって対応すること。
- (2) 本市が貸与または用意するものを除き、必要なものについては受注者が用意すること。

大分市立学校における情報セキュリティの基本方針

大分市教育委員会

1. 目的

本基本方針は、本市立小学校、中学校及び義務教育学校（以下「学校」という。）が保有する情報資産の機密性、完全性及び可用性を維持するため、学校における情報セキュリティ対策について基本的な事項を定めることを目的としています。

2. 定義

(1) 学校ネットワーク

学校のコンピュータ等を相互に接続するための通信網、その構成機器（ハードウェア及びソフトウェア）をいいます。

(2) 教育情報システム

学校のコンピュータ、学校ネットワーク及び電磁的記録媒体で構成され、情報処理を行う仕組みをいいます。

(3) 情報資産

本基本方針が対象とする情報資産は、次のとおりです。

- ①学校ネットワーク、教育情報システム、これらに関する設備、電磁的記録媒体
- ②学校ネットワーク及び教育情報システムで取り扱う情報（これらを印刷した文書を含む。）
- ③教育情報システムの仕様書及びネットワーク図等のシステム関連文書
- ④学校が保有し、校務及び授業において取り扱うすべての情報（紙等へ出力された情報を含む。）

(4) 情報セキュリティ

情報資産の機密性、完全性及び可用性を維持することをいいます。

①機密性

情報にアクセスすることが認められた者だけが、情報にアクセスできる状態を確保することをいいます。

②完全性

情報が破壊、改ざん又は消去されていない状態を確保することをいいます。

③可用性

情報にアクセスすることが認められた者が、必要なときに中断されることなく、情報にアクセスできる状態を確保することをいいます。

(5) 学校情報セキュリティポリシー

本基本方針及び大分市立学校における情報セキュリティ対策基準（以下「学校情報セキュリティ対策基準」という。）のことをいいます。

(6) 教職員等

情報資産にアクセスするすべての職員（臨時的任用又は非常勤の職にあるものを含む。）をいいます。

(7) 児童生徒

学校に在学している児童及び生徒をいいます。

(8) 外部委託事業者

業務委託等により情報資産を取り扱う業務に従事する事業者（下請けを行う者を含む。）をいいます。

(9) アクセス

情報資産に対し、何らかの利用目的を持って接触又は接続することで、帳票、簿冊等の記載内容を閲覧・転記するために接すること及び教育情報システムへネットワークを介したデータ取得のために端末を接続すること等をいいます。

3. 適用範囲

本基本方針が適用される範囲は、学校、教職員等及び情報資産とします。

4. 対象とする脅威

情報資産に対する脅威として、以下の脅威を想定し、情報セキュリティ対策を実施します。

- (1) 不正アクセス、ウイルス攻撃、サービス不能攻撃等のサイバー攻撃や部外者の侵入等の意図的な要因による情報資産の漏えい・破壊・改ざん・消去、重要情報の詐取、内部不正等
- (2) 情報資産の無断持ち出し、無許可ソフトウェアの使用等の規定違反、設計・開発の不備、プログラム上の欠陥、操作・設定ミス、メンテナンス不備、内部・外部監査機能の不備、外部委託管理の不備、マネジメントの欠陥、機器故障等の非意図的要因による情報資産の漏えい・破壊・消去等
- (3) 地震、落雷、火災等の災害によるサービス及び業務の停止等
- (4) 大規模・広範囲にわたる疾病による要員不足に伴うシステム運用の機能不全等
- (5) 電力供給の途絶、通信の途絶、水道供給の途絶等のインフラの障害からの波及等

5. 教職員等の責務

教職員等は、学校における情報セキュリティの重要性について共通の認識を持ち、業務の遂行に当たって学校情報セキュリティポリシー及び情報セキュリティ実施手順を遵守します。

6. 児童生徒への対応

教職員等は、児童生徒に授業又は教育以外の目的で情報資産を使用させないように、適切に指導します。

教職員等は、児童生徒が情報資産を使用するに当たり、あらかじめ情報セキュリティ対策上遵守すべき事項を明示した上で、適切に指導します。

7. 情報セキュリティ対策

脅威から情報資産を保護するために、以下の情報セキュリティ対策を実施します。

- (1) 組織・体制

学校における情報セキュリティ対策は、責任や役割を明確にした組織・体制の下に行うものとします。

(2) 情報の分類と管理

学校の保有する情報資産について、重要度に応じた情報分類の定義を行い、情報の管理責任及び管理方法を明確にします。

(3) 物理的セキュリティ

サーバ等、情報システム室等、通信回線等及び教職員等のパソコン等の管理について、物理的な対策を実施します。

(4) 人的セキュリティ

学校における情報セキュリティに関し、教職員等、児童生徒が遵守すべき事項を定めるとともに、十分な研修及び啓発を行う等の人的な対策を実施します。

(5) 技術的セキュリティ

コンピュータ等の管理、アクセス制御、不正プログラム対策、不正アクセス対策等の技術的対策を実施します。

(6) 運用

教育情報システムの監視、学校情報セキュリティポリシーの遵守状況の確認、外部委託を行う際のセキュリティ確保等、学校情報セキュリティポリシーの運用面の対策を実施します。

また、情報資産に対するセキュリティ侵害が発生した場合等に迅速かつ適正に対応するため、緊急時対応計画を策定します。

(7) 委託

外部委託する場合には、外部委託事業者を選定し、情報セキュリティ要件を明記した契約を締結し、外部委託事業者において必要なセキュリティ対策が確保されていることを確認し、必要に応じて契約に基づき措置を行います。

約款による外部サービスを利用する場合には、利用にかかる規定を整備し対策を講じます。

ソーシャルメディアサービスを利用する場合には、ソーシャルメディアサービスの運

用手順を定め、ソーシャルメディアサービスで発信できる情報を規定し、利用するソーシャルメディアサービスごとの責任者を定めます。

(8) 評価・見直し

学校情報セキュリティポリシーの遵守状況を検証するため、定期的又は必要に応じて情報セキュリティ監査及び自己点検を実施し、運用改善を行い情報セキュリティの向上を図ります。学校情報セキュリティポリシーの見直しが必要な場合は、学校情報セキュリティポリシーの見直しを行います。

8. 学校情報セキュリティポリシーの監査及び自己点検の実施

学校情報セキュリティポリシーの遵守状況を検証するため、定期的又は必要に応じて情報セキュリティ監査及び自己点検を実施します。

9. 学校情報セキュリティポリシーの見直し

情報セキュリティ監査及び自己点検の結果、学校情報セキュリティポリシーの見直しが必要となった場合及び情報セキュリティに関する状況の変化に対応するため新たに対策が必要になった場合には、学校情報セキュリティポリシーを見直します。

10. 学校情報セキュリティ対策基準の策定

上記、7、8及び9に規定する対策等を実施するために、具体的な遵守事項及び判断基準等を定める学校情報セキュリティ対策基準を策定します。

なお、学校情報セキュリティ対策基準は、公にすることにより本市の学校運営に重大な支障を及ぼすおそれがあることから非公開とします。

11. 情報セキュリティ実施手順の策定

学校情報セキュリティ対策基準に基づき、情報セキュリティ対策を実施するための具体的な手順を定めた情報セキュリティ実施手順を策定します。

なお、情報セキュリティ実施手順は、公にすることにより本市の学校運営に重大な支障

を及ぼすおそれがあることから非公開とします。

12. 公開範囲

本基本方針は、教職員等に対して学校の情報セキュリティ対策への指針を示すため、また市民・団体等に対して学校の情報セキュリティ対策への理解を得るため、広く公開を行うものとしします。

附 則

この基本方針は、平成22年4月1日から施行する。

附 則

この基本方針は、平成26年4月1日から施行する。

附 則

この基本方針は、平成29年4月1日から施行する。

附 則

この基本方針は、令和3年4月1日から施行する。

附 則

この基本方針は、令和7年4月1日から施行する。