

Sophia

HIGH SCHOOL

METaverse IMMERSIVE EDUCATION Risk Assessment

Academic year	2026 - 2027
Applies to	All students and staff at Sophia High School
Legal / statutory framework	KCSIE 2026
Prepared by	Katy Todd (DSL)
Approved by	Vanessa Temple
Date approved	1 August 2026
Review date	1 August 2027 (or as needed)

1. Purpose and Scope

This risk assessment identifies and manages the risks arising from delivering live and asynchronous lessons to pupils under the age of 18. It should be read alongside the school's Online Safety Policy, Child Protection & Safeguarding Policy, Data Protection Policy, Acceptable Use Policy and Anti-Bullying Policy.

2. Statutory and Regulatory Framework

This assessment has been prepared with direct reference to:

- Keeping Children Safe in Education (KCSIE) 2026 — in particular Part 1 (online safety, and the filtering and monitoring duty), Part 5 (child-on-child sexual harassment and violence), and the guidance on emerging online risks, including risks arising within game-based/virtual environments.
- UK GDPR and the Data Protection Act 2018, as amended by the Data (Use and Access) Act 2025 (DUAA), which introduces specific 'children's higher protection matters' for any online service likely to be accessed by children.
- The ICO's Age Appropriate Design Code (Children's Code) and its published guidance 'Children and the UK GDPR', which sets standards for data protection by design and default where children are users.
- The Online Safety Act 2023, relevant to the content-moderation and age-assurance obligations of the third-party platforms used.
- Working Together to Safeguard Children, referenced by KCSIE 2026 for multi-agency safeguarding practice.

Under DUAA 2025, before approving any platform likely to be accessed by children the school considers: how the provider protects and supports children using the service; whether children's data is used for profiling or direct marketing; and what age-assurance or parental-control mechanisms exist. This due diligence is recorded for each platform listed in Section 1.

3. Risk Rating Methodology

Each risk below is rated by combining the likelihood of the risk occurring with the potential impact if it does, using the matrix below. Ratings are reviewed at least annually and whenever a new platform is introduced.

Likelihood \ Impact	Low	Medium	High
Unlikely	Low	Low	Medium
Possible	Low	Medium	High
Likely	Medium	High	High

Risk Assessing Metaverse & Immersive Education – 2026-2027

To be viewed alongside the Esports Risk Assessment 2025-2026

Area/Facility	Risk Title	Risk Details	Risk Level	Impact	Control/Activities	Lead
Information Technology- Devices	Camera use on devices.	Cannot force background blur on student devices and teacher cannot turn pupil camera off- risk is inappropriate images and backgrounds being seen leading to a possible safeguarding concern. Learners may use AI-generated virtual backgrounds, avatars or manipulated images to conceal their surroundings or impersonate others, resulting in safeguarding concerns.	M	M	- Staff to be trained to be aware of scanning backgrounds of children. Staff should always be able to see student screens using split screen functions on their devices - Be vigilant to monitor children's environments - Manage call, end call immediately for all if high risk exposed in a home - Staff to report immediately - Staff maintain professional curiosity regarding changes in learners' appearance, behaviour and home environment. - AI-generated imagery or impersonation is reported immediately to the Designated Safeguarding Lead (DSL).	Teacher

Devices Management	Students being able to see each other-inappropriate contact through cameras or access outside of sessions	Possible inappropriate images shared on camera.	M	M	- Pupils to be taught how to use teacher expectations around usage - Parent guide shared for expectations of live lesson behaviour and camera use - Staff to be trained to be aware of scanning backgrounds during lessons of children - Teachers trained how to see students and their camera image during all parts of live lessons (e.g. Staff can use a second device or split screen to see children during the lesson) - Google Classrooms must have teacher present to start lesson/admit children - Learners must not record, livestream or share images or recordings from immersive learning sessions. - Personal messaging platforms (e.g. Discord, WhatsApp or Snapchat) must not be used to communicate with other participants unless authorised by the school. - Staff supervise all learner interactions throughout sessions.	Teacher/Education Team
VR Devices	Injury during use of VR Headset	Injury to students or damage to physical environment during VR Headset play Learners may experience motion sickness, dizziness, fatigue, sensory overload or physical injury whilst using VR equipment.	M	L	- Students provided with guidance for safe play zones + built in VR headset boundary. - Reminders by teachers to check your area of play - Provision of safety guidance - Learners advised to remove the headset immediately if feeling unwell. - Alternative 2D learning provided where appropriate. - Headsets cleaned between users. - Medical needs considered before participation.	Education Team
Persistent Environments	Staff leave the live lessons running for children to communicate in an unsupervised	Teachers and staff leave the lesson before seeing all of the pupils off of the session	L	L	- Teachers trained and guidance given on how to set up and use VR learning tools including lesson link, leaving and joining routines.	Education Team

	environment or encounter strangers	Strangers joining into sessions due to persistent metaverse settings			- EVC Risk Assessments used when taking children into persistent Metaverse environments - Private or invite-only environments used wherever possible. - Teacher remains present until all learners have exited. - Public access disabled. - Session links shared securely. - Teacher verifies participants before admission.	
Online Recordings	Screenshot or screen recording of children and staff from virtual lessons being misused	Pupil/Parent / external user screenshot the virtual lessons with pupil and teacher image on the screen for misuse and sending through media Learners may have screenshots, recordings, voice communications or avatar images captured, manipulated or redistributed without consent, resulting in cyberbullying, impersonation, data protection breaches or safeguarding concerns.	L	L	- Use of avatars / first name or code names only during vr sessions - Careful awareness and selection of a group/class so that teachers are aware of possible 'at risk' pupils (Safeguarding concerns) - AI manipulation of recordings treated as safeguarding concern. - Recordings stored securely. - Concerns reported immediately to DSL.	Teacher/ Education Team
Immersive Environments	Inappropriate language exposure during sessions	Unmuted mic allows pupils to misuse the session	L	L	- Pupils to be taught by their teachers ground rules around Metiquette expectations around language and usage - Parent guide shared for expectation and behaviour in digital lessons as part of digital safety agreement - Teacher controls for muting of participants or removal	Teacher/ Education Team
Security	Pupils password use- this can be shared by the pupil at home	Shared passwords or re-set passwords can mean that pupils could misuse system	L	L	- Pupils taught how to login with their Metaverse Platform credentials - Teacher shares code to enter platform in secure environment	Education Team / Teachers

		Learners may have accounts compromised through weak passwords, phishing attempts, credential theft or malicious software.			- Any updates to their accounts to be shared with parents and ICT Team - Strong passwords. - Multi-factor authentication where available. - Phishing awareness. - Only approved software installed. - Report compromised accounts immediately.	
Filtering and Monitoring	Filtering and monitoring systems	Learners may access harmful, inappropriate or illegal online content if filtering or monitoring systems fail to identify safeguarding concerns whilst using immersive learning platforms.	M	H	Appropriate filtering and monitoring systems. Alerts reviewed promptly. Staff understand system limitations. Concerns escalated to DSL. Systems reviewed regularly.	DSL/DPO/ICT Team
Online-Safety in Virtual Worlds	Chat facilities misused	Pupils use the chat in the VR session for inappropriate discussions with each other. Learners may be approached by unknown users or encouraged to communicate outside supervised learning environments.	M	L	- Teachers discuss chat expectations and record of all chats from all live lessons saved automatically - Recordings can be made available if needed for review which are emailed to teacher after each lesson - Learners never share personal information. - Learners never move conversations onto external platforms. - Staff monitor communications. - Concerns reported immediately.	Teacher
Remote Devices/Timings	Time Zone changes- this can be done by pupil at home	Pupil can change the time zones on device and therefore miss lessons.	L	L	- Teacher to make contact with parents to report any pupils who are absent from lessons if parents so not contact the teacher prior to the lesson - Attendance to live lessons guidance shared with parents	Teacher/ Education Team
Screen Time / Visual Issues	Children can spend too much time in VR / Gaming sessions damaging eyes	How much time is appropriate ? Do we know enough about	M	L	- Children can be provided with options to join 2D sessions - VR sessions linked to curriculum objectives with time frames set for time in VR	Teacher

		impact on eyesight and headsets on children Extended immersive learning may affect wellbeing, concentration, sleep, emotional regulation or physical comfort.			- Use where supports learning and don't where it doesn't - Planned breaks. - Wellbeing check-ins. - Appropriate session length. - Alternative learning available.	
Online-Safety	Children unable to keep themselves safe online	Pupils use search engines to access inappropriate sites whilst at home during lessons using Sophia High Account	H	M	- PSHE Curriculum- clear curriculum sequenced through year groups appropriateness on Online-Safety and keeping safe. - Learning Effectively Online unit taught annually across the school - Digital Safety lessons - Filtering and monitoring systems support safe online learning. - Staff understand limitations of filtering. - AI safety included within online safety curriculum. - Concerns escalated to DSL.	Teachers/ Education Team
Device Use	Damage of hardware from misuse/accidental water damage	Water damage from drinks and other items whilst devices are in use	H	M	- Pupils and parent guidance on not having open cup drinks close to the devices in lessons. Store at a safe distance.	Teachers
Avatar Dress Code	Pupils and parents in inappropriate dress code during VR sessions with Avatars	Over exposure of body parts, in appropriate clothing, image e.g. pyjamas. Offensive materials for local areas UAE Learners may create avatars, usernames or animations that are inappropriate, offensive or used to impersonate others.	M	L	- Pupils and parent guidance on netiquette for virtual lessons including avatar wardrobe selection. - Approved avatar standards. - Offensive names prohibited. - Impersonation prohibited. - Teacher monitors avatar appearance.	Teachers
Data Protection	Student data privacy & platform data storage	Metaverse platforms may store or collect personal data (e.g. voice, behavior, avatars), which may not	M	H	- Platforms must be GDPR-compliant; verify that data is stored securely within approved jurisdictions.	Education Team / Data Protection Officer

		comply with GDPR or local data protection policies. Learners may have personal information, voice communications, behavioural data, avatar information or other personal data collected, stored or shared inappropriately through immersive learning platforms, resulting in data protection breaches or safeguarding concerns.			- Data Protection Impact Assessment (DPIA) to be completed for each new platform. - Parents to be informed and give written consent for data sharing and storage. - Limit personal data collection—only first names or pseudonyms used in sessions. - Any suspected data breach reported immediately in accordance with the school's Data Protection and Safeguarding policies.	
Artificial Intelligence (AI)	AI-generated content and impersonation	Learners may encounter or create AI-generated avatars, images, voice recordings, videos or messages that are misleading, inappropriate, harmful or used to impersonate others, resulting in bullying, harassment or safeguarding concerns.	M	M	Learners taught safe and ethical use of AI. Staff trained to recognise AI-generated content. AI misuse treated as safeguarding concern. Concerns reported immediately to DSL. Parents informed where appropriate.	Teacher/Education Team
Staff Use of Artificial Intelligence (AI)	Staff Use of Artificial Intelligence (AI)	Staffs and Learners' personal information or safeguarding information may be unintentionally disclosed if staff use unapproved or public AI tools, resulting in data protection breaches or safeguarding concerns	M	H	Staff must not enter confidential, personal or safeguarding information into publicly available AI tools. Staff follow the school's AI, Data Protection and Safeguarding policies. Staff receive training on the safe, ethical and appropriate use of AI. Only school-approved AI platforms and applications are used for educational purposes.	SLT / DSL / DPO
Monitoring & Evaluation	Overuse or ineffective use of immersive Tools	Over-reliance on immersive tools may impact learning or wellbeing without measured outcomes.	L	L	- Termly reviews of VR lesson outcomes and student engagement. - Parent and pupil surveys to evaluate impact.	Education Team / SLT

					- Use immersive tools only when clearly linked to curriculum objectives.	
--	--	--	--	--	--	--

5. Roles and Responsibilities

Designated Safeguarding Lead DSL, DDSL and EDDSL	Overall responsibility for e-safety risk management, incident logging and liaison with external safeguarding partners under KCSIE 2026.
Data Protection Officer (DPO)	Reviews DPIAs for new platforms; ensures compliance with UK GDPR, DPA 2018 and DUAA 2025 children's higher-protection requirements.
IT Lead	Manages device provisioning, filtering and monitoring systems, MDM and platform access/room security.
Class Teacher (session host)	Live supervision, moderation of submissions, management of room codes and immediate response to in-session incidents.
Governing Body / Proprietor	Approves this risk assessment and monitors implementation through the school's standing safeguarding reporting arrangements.

7. Review and Sign-off

This risk assessment will be reviewed at least annually, on publication of a revised KCSIE edition, following any relevant change in data protection law, or immediately following any e-safety incident involving one of the platforms listed.

Prepared by	Katy Todd (DSL)
Reviewed by (DPO)	Fernando Darcie (DPO)
Approved by (Headteacher/Governors)	Vanessa Temple
Next review due	August 2027