

Sophia

HIGH SCHOOL

Esports Education – Risk Assessment 2026-2027

<u>Academic year</u>	2026-2027
<u>Applies to</u>	All staff and students of Sophia High School and Sophia Technologies
<u>Legal / statutory framework</u>	KCSIE 2026
<u>Prepared by</u>	Katie Todd (DSL)
<u>Approved by</u>	Fernando Darcie (DPO)
<u>Date approved</u>	August 2026
<u>Review date</u>	August 2027

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.

<u>Likelihood \ Impact</u>	<u>Low</u>	<u>Medium</u>	<u>High</u>
<u>Unlikely</u>	<u>Low</u>	<u>Low</u>	<u>Medium</u>
<u>Possible</u>	<u>Low</u>	<u>Medium</u>	<u>High</u>
<u>Likely</u>	<u>Medium</u>	<u>High</u>	<u>High</u>

4. Risk Assessment

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 of inappropriate images and backgrounds being seen leading to a possible safeguarding concern. Staff maintain professional curiosity regarding changes in	L	M	Staff should: - Be trained to be aware of and how to scan backgrounds of children. - 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 is exposed.	Teacher

		learners' presentation, behaviour and home environment.			- Report concerns immediately, following Safeguarding policy.	
Devices Management	Students being able to see each other, inappropriate content through cameras, or access to online areas outside of sessions.	Possible inappropriate images or content shared on camera or by other means, or access to unsupervised areas (chat rooms etc.)	M	M	- Students to be taught and understand expectations around use and be aware of safeguarding concerns and actions to keep themselves safe. - Parent guide shared for expectations of live session behaviour and camera use. - Staff to be trained to be aware of scanning backgrounds during lessons with children. - Staff 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 a Teacher present to start lessons/admit children, and remain in the spaces for monitoring.	Teacher / Education Team
Online Recordings	Screenshot or screen recording of children and staff from virtual lessons being misused. AI manipulation, redistribution	Pupil/Parent or external user screenshot of the virtual lessons with pupil and teacher image on the screen for misuse and sending through media without permissions or in breach of Safeguarding regulations.	L	M	- Understanding of Safeguarding policy and procedures, and how they relate to their actions and responsibilities in online spaces. - Awareness by all students of risks and how to mitigate them. - Use of avatars / first name or code names only during Esports sessions.	Teacher / Education Team

	and impersonation.					
Data Protection	Student data privacy and platform data storage	Learners may have personal information, gaming identities, recordings, voice communications or other personal data collected, stored or shared inappropriately through gaming or competition platforms, resulting in data protection breaches or safeguarding concerns.	M	H	GDPR-compliant platforms. DPIA completed. Minimum personal information. Secure recordings. Data breaches reported. Remedial and preventive actions are taken.	Education Team / DPO
Immersive Environments	Inappropriate language exposure during sessions.	Unmuted mic allows students to misuse the session. Different expectations from participants, unsure of expected standard of language.	L	L	- Students to be taught by their teachers ground rules around etiquette 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 if language continues.	Teacher/ Education Team
Security	Pupil passwords shared with others by the pupil at home.	Shared passwords or reset passwords can mean that students and others could misuse the system. Danger of non-authorised access to restricted or secure areas. phishing compromised accounts	L	L	- Students taught how to login with their Minecraft Education credentials. - Teacher shares code to enter the platform in a secure environment. - Any updates to their accounts to be shared with parents and ICT Team to retain confidential access. MFA where available phishing awareness	Education Team / Teachers / ICT Team

		malicious downloads credential theft			approved software only compromised accounts reported immediately	
Filtering & Monitoring	Filtering and monitoring systems fail to identify harmful online activity.	Learners may access harmful, extremist, sexual, violent or otherwise inappropriate content if filtering or monitoring systems fail to identify safeguarding concerns whilst using school technology or online platforms.	M	H	Appropriate filtering and monitoring systems. Staff understand limitations. Alerts investigated promptly. Concerns reported to DSL. Systems reviewed regularly	ICT Team / DSL
DeviceUse	Misuse / accidental water damage of hardware.	Water damage from drinks, food or other items whilst devices are in use.	M	H	- Students/Parents/Guardians are aware of how to keep equipment safe and working optimally. - No open drinks or food close to the devices. Store at a safe distance.	Teacher
Screen Time / Visual Issues	Children can spend extended periods in gaming sessions, damaging eyesight.	Extended screen use may affect visual comfort, sleep, concentration and wellbeing. Appropriate breaks are incorporated into lessons.	H	H	- Screen time is monitored by an adult and students understand the health risks of extended screen time. - Students are required to take regular breaks from screen time. - Independent learning for school can be completed without using a computer or other electronic device to help reduce screen time.	Teacher
Online Safety	Children unable to keep themselves safe online.	Students are unaware of the Safeguarding Policy and Procedures. Students have not signed the Digital Agreement and are not aware of safety expectations. They use search engines to access inappropriate sites whilst at home,	L	H	- PSHE Curriculum (Holistic Horizons), sequenced through year groups will address online safety as required by <u>DfE</u> . - Appropriate schedule of lessons on online safety and keeping safe online as recorded on the school calendar, including student and parent workshops.	Teachers/ EducationTeam

		during lessons using their Sophia High School account.			-Learning Effectively Online unit taught annually across the school at the beginning of the school year. - Digital Safety lessons, as appropriate for student age and skills, identified throughout the year.	
Online Safety in Virtual Worlds	Chat facilities accessed without authorisation and/or misused.	Students use the chat in the Minecraft session for inappropriate discussions with others. Unauthorised and unknown others accessing the chat facility, could lead to inappropriate discussion or relationships. Learners should never move conversations onto personal messaging platforms (Discord, WhatsApp, Snapchat etc.).	L	L	- Teachers discuss chat expectations and records of all chats from all live lessons are saved automatically. - Recordings can be made available if needed for review which are emailed to the teacher after each lesson.	Teacher
Remote Devices / Timings.	Time zone changes - this can be done by students at home	Students can change the time zones on their devices and therefore miss lessons.	L	L	- Teachers/Admissions to contact parents to report any students who are absent from lessons. - Attendance to live lessons expectations shared with parents as set by the DfE.	Teacher/ Education Team
In-Game Skins / Avatar	Learners may set inappropriate Minecraft skins	Learners can set custom Minecraft skins to their accounts which may feature inappropriate imagery or content (e.g. depiction of nudity or offensive weapons)	L	L	- Students made aware of the expectations and consequences of breach of acceptable conduct. - Maps always set to have only approved skins displayed to prevent custom (potentially inappropriate) skins being shown.	Teacher

Artificial Intelligence (AI)	AI-generated content and impersonation	Learners may encounter or create AI-generated images, videos, voice recordings, avatars or messages that are misleading, inappropriate, harmful or used to impersonate others, resulting in bullying, harassment or safeguarding concerns.	M	M	Safe and ethical AI taught. Staff trained to recognise AI-generated content. AI misuse treated as safeguarding concern. Concerns reported to DSL. Parents informed where appropriate.	Teacher / Education Team
Artificial Intelligence (AI)	Staff use of AI	Staff 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	No confidential safeguarding information entered into public AI systems. Staff follow AI policy. Approved AI only. Staff training.	SLT / DSL / DPO
Curriculum	Mature nature of course content	Certain core aspects of the course contain mature content which may be distressing or inappropriate for certain learners. E.G. looking at 18 rated games that are industry leaders such as Counter Strike and Call of Duty.	M	L	Pupils to be told in advance when mature content will be planned to be discussed. Staff to restrict content of age restricted materials to discussions and avoid graphic imagery, including photos, videos and live demonstrations.	Teacher / Education Team

Supervision of Breakout Rooms and Collaborative Online Learning

Breakout rooms are an integral part of the school's delivery model, enabling paired and small-group collaborative work in line with the pedagogy of the Online Learning Policy. The school's approach to safeguarding within breakout rooms **follows the principles of Keeping Children Safe in Education: supervision that is reasonable, proportionate and appropriate to the setting, rather than continuous surveillance of every pupil interaction — the same standard that applies to group work, corridors and shared spaces in a physical school.**

The following controls apply whenever breakout rooms are in use: · The class teacher retains host control of the whole session at all times, remains present in the lesson throughout, and moves between breakout rooms on an unannounced basis, as a teacher would circulate between groups in a physical classroom.

The class teacher retains the ability to recall all students immediately to the main classroom where this is necessary for safeguarding, behaviour management or teaching purposes.

Where safeguarding, behaviour or welfare concerns arise, staff may close breakout rooms immediately, return students to the main classroom and take any further action necessary in accordance with the school's Safeguarding and Child Protection Policy and Behaviour Policy.

Staff remain professionally curious regarding learners' interactions, behaviour, presentation and any disclosures arising from breakout room activities, following up any concerns in accordance with the school's Safeguarding and Child Protection Policy.

Breakout groups are kept deliberately small, consistent with the school's small-group model.

- Every pupil retains an immediate exit at all times: any pupil may leave a breakout room and return to the main room, or leave the lesson entirely, at any moment. Pupils learn from home, with a parent or carer contactable as set out in the Online Learning Policy.
- All pupils are taught, and sign an age-appropriate Digital Safety Agreement committing to, the expectation that they report immediately to an adult anything that makes them uncomfortable, in a breakout room or anywhere else online. The school's behaviour and anti-bullying expectations apply in breakout rooms exactly as they do in the main classroom and in a physical school.
- Concerns raised about conduct in breakout rooms — by a pupil, parent or member of staff — are followed up promptly under the school's Safeguarding and Child Protection Policy and Behaviour Policy, and grouping arrangements may be adjusted while any concern is looked into.
- Structured weekly parent contact provides a regular, reliable route through which concerns about peer interactions are surfaced and acted upon.

The school keeps its arrangements for breakout rooms and collaborative learning under continuous review as part of its safeguarding risk assessment, annual policy review cycle and in response to emerging safeguarding risks, technological developments and updates to statutory guidance.

5. Roles and Responsibilities

Designated Safeguarding Lead DSL, DDSL and EDDSL	Overall responsibility for online 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.

6. 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 online safety incident involving one of the platforms listed.

Prepared by	Katie Todd (DSL)
Reviewed by (EDDSL)	Tyler Wilson (EDDSL)
Reviewed by (DPO)	Fernando Darcie (DPO)
Approved by (Headteacher/Governors)	Vanessa Temple
Next review due	August 2026