

Sophia HIGH SCHOOL

**Safeguarding in Esports Education
2026 - 2027**

SAFEGUARDING IN ESPORTS EDUCATION

Ownership & Consultation	
Document sponsors (role)	CEO / Director of Education
Document authors (name)	Tyler Wilson, Esports Lead, EDDSL Vanessa Temple, Director of Education Melissa McBride, CEO Fernando Darcie, DPO

Version control	
Implementation date	September 2024
Reviewed and updated	August 2025
Reviewed and updated	August 2026
Review Date	August 2027

Safeguarding in Esports Education

Introduction and Context

As Sophia High School embraces innovative educational opportunities, we recognise the growing significance of Esports within both education and future career pathways. This addition to our Safeguarding Policy addresses the specific considerations and protective measures required to ensure pupil safety within Esports education, whilst maintaining alignment with our statutory safeguarding obligations under Keeping Children Safe in Education.

The rapid evolution of the gaming and Esports sector presents both opportunities and challenges within educational settings. As we integrate Esports into our curriculum, we maintain our paramount commitment to safeguarding, acknowledging that this emerging field requires specific protective measures alongside our established safeguarding framework.

As an online school, Sophia High School recognises that many safeguarding concerns arising within Esports education mirror wider online safety risks and will therefore be managed through the School's safeguarding, digital safety and behaviour procedures where appropriate.

Key People and Contacts

- Designated Safeguarding Lead - Katy Todd - katy.todd@sophiahigh.school
- Deputy Designated Safeguarding Lead - Nicki Pelletier - [Nicki Pelletier](#)
- Esports-Designated Safeguarding Lead and Head of Esports - [Tyler Wilson](#)

Contacts for Statutory Bodies

National Society for the Prevention of Cruelty to Children - <https://www.nspcc.org.uk/>

UK Safer Internet Centre - <https://saferinternet.org.uk/>

Childnet - <https://www.childnet.com/>

British Esports Federation - <https://britishesports.org/contact-us/>

Keeping Children Safe in Education (2026): [Keeping Children Safe in Education \(2026\)](#)

Department for Education – Working Together to Safeguard Children 2026: [Working Together to Safeguard Children 2026](#)

UKCIS – [Education for a Connected World](#)

UKCIS – [Sharing Nudes and Semi-Nudes: Advice for Education Settings Working with Children and Young People \(2024\)](#)

Filtering and Monitoring Standards for Schools and Colleges (2022), (Updated 2026): [Filtering and Monitoring Standards for Schools and Colleges \(2022\), \(Updated 2026\)](#)

Safeguarding Principles in Esports Education

Our approach to Esports safeguarding integrates seamlessly with our existing online safety measures and whole-school safeguarding procedures. We recognise that Esports environments present unique considerations that align with the four key areas of risk identified in Keeping Children Safe in Education:

Content: Pupils may be exposed to inappropriate gaming content, aggressive behaviour, or harmful messaging within gaming platforms.

Contact: The interactive nature of Esports can expose pupils to unknown contacts, potential grooming, or inappropriate communication. The School recognises that some gaming and online communities may expose young people to extremist content, harmful ideologies or radicalising influences. Concerns will be managed in accordance with the School's Prevent Duty procedures.

Staff will remain alert to misogynistic attitudes, harmful sexual behaviour and online content that may promote violence, hatred or discrimination against women and girls. Concerns will be addressed in accordance with the school's Safeguarding and Child Protection Policy and relevant behaviour and online safety procedures.

Conduct: Pupils may experience or engage in harmful online behaviour, including cyberbullying, excessive gaming, or inappropriate competitive conduct.

Commerce: The growing monetisation of gaming presents risks around in-game purchases, gambling-like mechanics, and commercial exploitation. This includes awareness of loot boxes, gambling-like mechanics, microtransactions and other monetised features which may present financial or wellbeing risks for children and young people.

Integration with Existing Safeguarding Measures

This policy addition builds upon our established safeguarding framework, ensuring that Esports activities maintain the same rigorous standards of pupil protection applied across all areas of school life. Our approach recognises that Esports activities, while innovative and engaging, must operate within a comprehensive safeguarding environment that:

- Maintains robust monitoring and supervision protocols specific to online gaming environments
- Ensures appropriate adult oversight of all Esports activities and communications
- Implements clear reporting procedures for concerns arising within Esports contexts
- Provides specific training for staff involved in Esports education
- Establishes clear boundaries between educational gaming and recreational activities
- Supports parents in understanding and monitoring their children's engagement with Esports

Staff involved in Esports provision will receive safeguarding updates reflecting changes to KCSIE, DfE online safety guidance, emerging gaming risks, AI-generated content, harmful sexual behaviour, child-on-child abuse, misogyny and relevant Prevent risks.

SAFEGUARDING IN ESPORTS EDUCATION

Commitment to Safe Educational Innovation

As we embrace Esports as an educational pathway, we remain committed to creating a safe, supportive environment that protects pupils while fostering their engagement with emerging technologies and career opportunities. This policy recognises that effective safeguarding in Esports requires a dynamic approach that evolves alongside technological advancement and industry developments.

The following sections detail specific measures, procedures, and guidelines implemented to ensure that our Esports provision maintains the highest standards of pupil safety and wellbeing, in accordance with our statutory obligations and commitment to exemplary safeguarding practice.

Educational Purpose and Career Development

In developing our Esports provision, Sophia High School recognises its responsibility to prepare pupils for future opportunities while ensuring their safety and wellbeing. Recent research indicates that 40% of Generation Z are considering careers in video game-related fields, with more than 20% specifically interested in Esports roles. This significant shift in career aspirations requires careful consideration within our safeguarding framework.

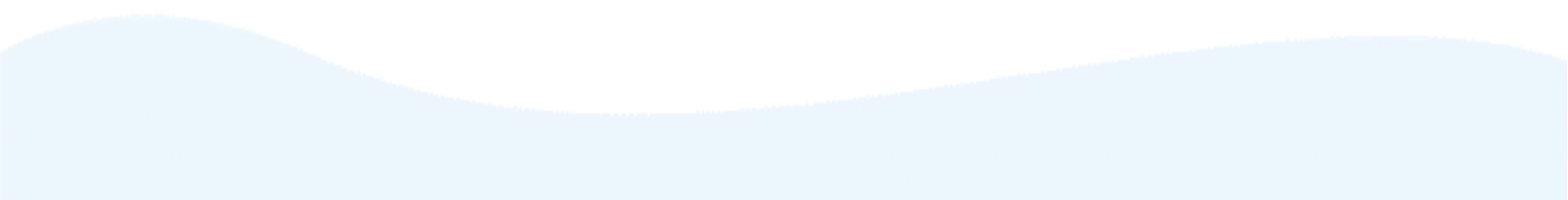
Our approach acknowledges that while Esports presents valuable educational and career development opportunities, these must be balanced with robust safeguarding measures. The integration of Esports into our curriculum reflects our commitment to innovative education while maintaining our duty of care. This includes:

Structured Career Guidance: We provide supervised exposure to Esports career pathways, ensuring that career exploration occurs within protected educational environments. This includes carefully monitored interaction with industry professionals and structured learning about career opportunities.

Skills Development Framework: Our programme develops transferable skills including digital literacy, strategic thinking, and teamwork, while maintaining appropriate boundaries and safeguards. All skill development activities are designed with embedded protective measures.

Industry Engagement Protocols: When engaging with the gaming industry for educational purposes, we implement strict vetting procedures and supervisory protocols. This ensures that industry exposure enhances learning while protecting pupils from potential risks.

Digital Citizenship Education: Alongside Esports skills, we emphasise responsible online behaviour, digital wellbeing, and safe gaming practices. This includes education about online risks, appropriate competitive behaviour, and healthy gaming habits.



Educational Integration and Safeguarding Measures

The integration of Esports into our curriculum represents a carefully considered approach that balances educational innovation with robust safeguarding protocols. Each aspect of our Esports provision is designed to protect pupils whilst delivering meaningful educational outcomes.

Curriculum Integration and Safety Our STEAM-integrated Esports curriculum operates within strict safeguarding parameters. When mathematical concepts are explored through gaming strategies or storytelling skills are developed through interactive narratives, staff maintain constant oversight to ensure appropriate content and interaction. All digital platforms and games used for educational purposes undergo rigorous safety assessment and continuous monitoring.

Protected Learning Environments The delivery of Esports education occurs within carefully controlled digital environments. Our technical infrastructure includes:

- Secured gaming platforms with appropriate content filters
- Monitored communication channels
- Regular safety audits of all digital learning spaces
- Implementation of age-appropriate restrictions

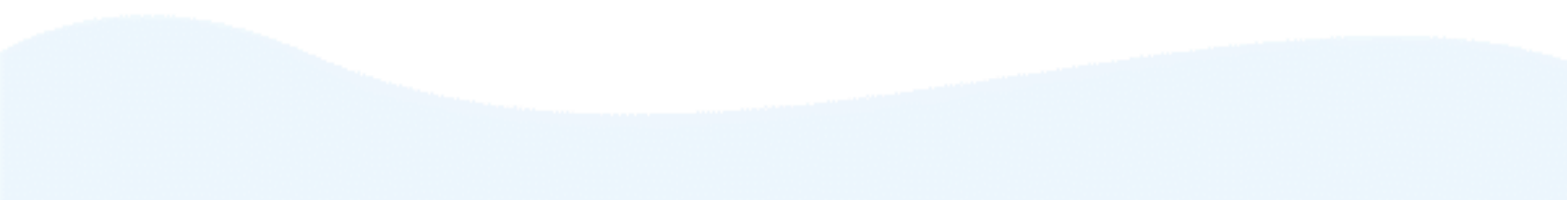
Engagement and Wellbeing Whilst Esports provides valuable engagement opportunities for pupils who may not participate in traditional activities, we maintain vigilant oversight of participation patterns. Staff are trained to:

- Monitor for signs of excessive gaming or addictive behaviours
- Ensure balanced participation across activities
- Maintain appropriate boundaries between educational and recreational gaming
- Support healthy gaming habits and digital wellness

STEAM Skills Development The development of technical skills through Esports is conducted with comprehensive safety measures in place. When pupils engage in coding, game development, or mathematical applications, we ensure:

- Secure development environments
- Protected collaborative spaces
- Monitored peer interaction
- Regular safety reviews of all technical tools

Social and Emotional Development The social and emotional growth opportunities within Esports are supported by clear safeguarding protocols. Our approach includes:

- Structured teamwork activities with appropriate supervision
 - Monitored communication channels for collaborative work
 - Regular assessment of online interactions
 - Clear guidelines for respectful competitive behaviour
- 

SAFEGUARDING IN ESPORTS EDUCATION

College and Career Preparation As pupils explore potential career pathways in Esports, we maintain strict safeguarding measures around industry engagement. This includes:

- Vetted professional interactions
- Supervised industry exposure
- Protected networking opportunities
- Secure career development activities

These educational opportunities are delivered within our comprehensive safeguarding framework, ensuring that all activities maintain appropriate protections for our pupils. Staff receive specific training in identifying and managing risks associated with Esports education, while supporting pupils in exploring these emerging career pathways safely.

Digital Delivery and Safeguarding Implementation

The delivery of Esports education at Sophia High School occurs within our established digital-first learning environment, incorporating comprehensive safeguarding measures specifically designed for remote education. As an online school, we have developed robust protocols that ensure the secure delivery of Esports education while maintaining the highest standards of pupil protection.

Professional Oversight and Delivery Our Esports provision is led by qualified teachers who possess both educational expertise and specialist industry experience. These professionals undergo enhanced safeguarding training specific to online gaming environments and remote education. This dual expertise ensures that educational content is delivered with a thorough understanding of both gaming culture and online safety requirements.

Secure Digital Learning Environments The cornerstone of our Esports delivery is our carefully controlled digital infrastructure. Within platforms such as Minecraft Education Edition, we create secure, education-specific environments that function as protected virtual classrooms. These spaces are:

- Designed and maintained by Sophia High School teachers in collaboration with Microsoft education specialists
- Accessed through unique, randomised join codes issued individually to enrolled pupils
- Continuously monitored through sophisticated digital oversight tools
- Regularly audited for security compliance and educational appropriateness

Protected Communication Channels All communication within our Esports provision occurs through monitored, education-specific channels. Our systems ensure:

- Secure teacher-student communication pathways
- Monitored peer interaction spaces
- Recording and oversight of all digital interactions
- Regular review of communication protocols

Comprehensive Digital Safeguarding Our remote delivery model incorporates multi-layered safeguarding measures:

- Monitoring and oversight will be proportionate to the identified safeguarding risks and the capabilities of the relevant platform. Monitoring systems and staff oversight are used to identify and respond to safeguarding concerns within the Esports environment.
- Secure authentication protocols for all participants

SAFEGUARDING IN ESPORTS EDUCATION

- Regular safety assessments of digital platforms
- Clear procedures for reporting concerns
- Immediate intervention capabilities for teaching staff

Integration with STEAM Curriculum As part of our wider STEAM curriculum and Gaming Innovators programme, Esports is delivered within an established educational framework. This integration ensures:

- Alignment with academic standards and learning objectives
- Regular assessment of educational outcomes
- Continuous evaluation of safeguarding effectiveness
- Integration with wider digital safety education

Mobile phones and personal devices are subject to the school's Mobile Phone and Personal Device Policy. Where personal devices are permitted for an identified educational purpose within Esports activities, their use will be authorised, age-appropriate, safeguarded and subject to the school's acceptable-use, filtering, monitoring and data-protection arrangements.

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.

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.

SAFEGUARDING IN ESPORTS EDUCATION

- 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.

Parent and Guardian Engagement

Our remote delivery model includes specific provisions for parent and guardian involvement:

- Regular updates on Esports activities and safety measures
- Clear communication about digital safety protocols
- Guidance on supporting safe gaming practices at home
- Opportunities for feedback and concerns

These measures ensure that our digital-first approach to Esports education maintains the highest standards of pupil safety while delivering innovative learning experiences. Our safeguarding frameworks are continuously reviewed and updated to reflect emerging best practices in online education and digital safety.

These educational opportunities are delivered within our comprehensive safeguarding framework, ensuring that all activities maintain appropriate protections for our pupils. Staff receive specific training in identifying and managing risks associated with Esports education, while supporting pupils in exploring these emerging career pathways safely.

Types of Safeguarding Concerns for Esports Education

There are many types of safeguarding concerns that will present themselves when discussing esports education. These include:

1. Online Environment Risks
 - Potential exposure to inappropriate content
 - Cyberbullying
 - Unauthorised access to private spaces
 - Communication with unknown individuals
2. Competition-Related Risks
 - Online interaction with external participants
 - Potential for inappropriate communication
 - Mental health and well-being concerns during competitive events

SAFEGUARDING IN ESPORTS EDUCATION

3. Technical Safety Concerns

- Data privacy and protection
- Age-appropriate content filtering
- Secure access management

Child-on-child abuse and harmful behaviour

- Bullying and cyberbullying
- Sexual harassment or harmful sexual behaviour
- Coercion, intimidation or exploitation
- Non-consensual sharing of images or recordings
- Misogynistic or discriminatory online behaviour
- AI-generated or manipulated content used to harm another pupil

AI-Generated Content Risks

Pupils may encounter or create AI-generated images, videos, voice recordings or other synthetic media within gaming and online environments. The creation, sharing or distribution of AI-generated content that causes harm, distress, bullying, harassment, discrimination or safeguarding concerns will be treated as a safeguarding matter and managed in accordance with the School's Safeguarding Policy.

Staff will also remain alert to AI-generated or manipulated content, including deepfakes, that may constitute bullying, harassment, sexual abuse, exploitation or other safeguarding concerns.

Identification and Management of Safeguarding Risks

The delivery of Esports education in a digital environment presents specific safeguarding considerations that require robust management protocols. Sophia High School maintains comprehensive procedures for identifying, preventing, and addressing potential risks within our Esports provision (see RISK ASSESSMENTS – Appendix 1 and 2).

Online Environment Safety

Our digital learning spaces operate under strict safety protocols designed to protect pupils from online risks. The school implements multiple layers of protection to create secure educational environments. Teaching staff maintain continuous oversight of all digital interactions, supported by automated monitoring systems that flag potential concerns for immediate review.

Access to all Esports learning environments is strictly controlled through our secure authentication system. Each session operates with unique access credentials, ensuring that only registered pupils and authorised staff can participate. We maintain detailed logs of all digital interactions, enabling swift investigation of any concerns that may arise.

Competition and Event Management

Participation in competitive Esports events requires additional safeguarding measures. Before any external competition, we conduct thorough risk assessments considering both digital and wellbeing factors. Our competition protocols include:

SAFEGUARDING IN ESPORTS EDUCATION

Pre-event safety briefings for all participants and staff
Continuous monitoring of all communication channels during events
Clear procedures for managing inappropriate behaviour or communication
Regular wellbeing checks throughout competitive activities
Post-event debriefing sessions to identify any concerns

Technical Infrastructure and Data Protection

Our technical infrastructure incorporates comprehensive safety measures to protect both pupil data and online interactions. We maintain robust firewalls and content filtering systems specifically configured for educational gaming environments. Regular security audits ensure the continued effectiveness of these protective measures.

Data protection protocols align with GDPR requirements and educational best practices, ensuring secure handling of all pupil information. Technical systems undergo regular testing and updating to address emerging security challenges.

The school will assess whether its filtering and monitoring arrangements are effective in identifying and managing risks arising from real-time, dynamic, personalised and AI-generated content used within Esports platforms and related digital environments. Such risks will be considered as part of the school's annual filtering and monitoring review and wider safeguarding risk assessment.

Cyber Security and Safeguarding

Cyber security is recognised as an integral part of safeguarding within the school's digital-first Esports provision. The school will maintain appropriate technical and organisational measures to protect pupil information, secure access to Esports platforms, reduce the risk of unauthorised access and respond to cyber security incidents in accordance with the school's cyber security, data protection and safeguarding procedures.

Response Procedures and Support Systems

The school maintains clear response procedures for addressing safeguarding concerns within Esports activities. When concerns arise, our protocols ensure:

Immediate Assessment: Staff are trained to quickly evaluate potential risks and implement appropriate protective measures.

Swift Intervention: Clear procedures enable immediate response to any safeguarding concerns, including the ability to suspend activities if necessary.

Comprehensive Recording: All incidents and concerns are thoroughly documented through our secure reporting system.

Appropriate Escalation: Clear pathways exist for escalating concerns to senior safeguarding staff and external agencies when required.

Staff should understand that data protection and confidentiality must not prevent the sharing of information where sharing is necessary to safeguard and protect a child. Information will be shared lawfully, proportionately and on a need-to-know basis, in accordance with the school's Safeguarding and Child Protection Policy and information-sharing procedures.

SAFEGUARDING IN ESPORTS EDUCATION

Student Wellbeing Support

Our safeguarding framework includes comprehensive support for pupil wellbeing within Esports activities. This encompasses:

Digital Wellness Education: Regular sessions on maintaining healthy gaming habits and digital balance.

Mental Health Support: Access to qualified support staff for addressing competition-related stress or concerns.

Peer Support Systems: Structured programmes to promote positive gaming culture and mutual support among pupils.

Continuous Review and Development

Our safeguarding measures undergo regular review and updating to address emerging challenges in the digital gaming environment. This includes:

Annual Risk Assessment Reviews: Comprehensive evaluation of all Esports activities and safety protocols.

Regular Policy Updates: Integration of new safety measures and best practices as they develop.

Staff Training: Ongoing professional development in digital safety and Esports safeguarding.

CPD qualification with certificate: Duty to Care provided by the British Esports Federation

These comprehensive safeguarding measures ensure that our Esports provision maintains the highest standards of pupil safety while delivering engaging educational experiences. Through careful monitoring, swift response procedures, and robust support systems, we create a secure environment for pupils to develop their skills and knowledge in this emerging field.

These educational opportunities are delivered within our comprehensive safeguarding framework, ensuring that all activities maintain appropriate protections for our pupils. Staff receive specific training in identifying and managing risks associated with Esports education, while supporting pupils in exploring these emerging career pathways safely.

Filtering and monitoring arrangements will be reviewed at least annually by the relevant senior leader, DSL and IT/technical support, with the review recorded and any identified actions tracked to completion.

Responses to Concerns for Esports Education

We update our Risk Assessments for Esports (internal) and Esports (external competitions) annually, with additional updates as needs indicate.

There are many interventions for preventing and dealing with concerns within esports education. These include:

1. Immediate Reporting Procedure

- Clear protocol for students to report any uncomfortable or inappropriate interactions

SAFEGUARDING IN ESPORTS EDUCATION

- Confidential reporting mechanisms
- Rapid response and investigation process
- 2. Risk Mitigation Strategies
 - Comprehensive risk assessments for all online educational activities
 - Parental consent and communication
 - Ongoing monitoring of online spaces
 - Adherence to hosting entities' policies during competitions
- 3. Student Support
 - Access to SHS support services
 - Digital literacy and online safety education
 - Clear guidelines for online behavior
- 4. Where Esports-related safeguarding concerns involve a pupil who is questioning their gender, staff will follow the school's Safeguarding and Child Protection Policy and the relevant KCSIE guidance.

Initial Safeguarding Certification

Before any engagement with pupils, all staff members must complete a comprehensive suite of safeguarding certifications. This mandatory preparation encompasses advanced training in child protection within digital environments, with particular emphasis on the unique challenges presented by online gaming and competitive Esports. Staff must demonstrate proficiency in recognising and responding to potential risks, including child exploitation, self-harm indicators, and mental health concerns. They must also complete the Duty to Care certification from the British Esports Federation.

The initial certification process requires successful completion of specialised modules covering digital safeguarding principles, age-appropriate gaming guidance, and emergency response protocols. Staff must achieve certification in suicide prevention and safety planning, ensuring they possess the necessary skills to support pupil wellbeing in high-pressure competitive environments.

The effective delivery of safe Esports education relies fundamentally on the expertise and vigilance of our staff. Sophia High School maintains rigorous training requirements to ensure all personnel involved in Esports provision possess the necessary skills and knowledge to safeguard pupils effectively in digital environments.

SAFEGUARDING IN ESPORTS EDUCATION

Professional Development and Staff Training

Our commitment to safeguarding excellence requires continuous professional development throughout the academic year. Staff engage in regular training sessions that address emerging challenges in digital safety and Esports education. These sessions incorporate real-world scenarios and case studies, enabling staff to develop practical skills in identifying and managing potential risks.

The ongoing training programme includes quarterly updates on emerging online safety trends, evolving gaming platforms, and new safeguarding best practices. Staff participate in collaborative learning sessions, sharing experiences and insights to strengthen our collective safeguarding capabilities.

Practical Implementation Training

Our professional development programme emphasises practical application through scenario-based learning. Staff regularly participate in simulated incidents and response exercises, ensuring they maintain the skills necessary to address safeguarding concerns effectively. These practical sessions cover various situations, from managing inappropriate online behaviour to responding to technical security breaches.

Digital Environment Expertise

Staff receive specialised training in managing digital learning spaces, with particular focus on monitoring online interactions and maintaining secure gaming environments. This includes advanced instruction in:

Understanding digital behaviour patterns and potential indicators of concern
Managing appropriate boundaries in online educational settings
Implementing effective monitoring protocols for gaming platforms
Responding swiftly to technical security concerns

Documentation and Assessment

All staff training is thoroughly documented and regularly assessed to ensure consistent high standards across our Esports provision. Staff members maintain professional development portfolios that record their training completion, assessments, and ongoing learning needs. Regular evaluation ensures that training remains relevant and effective in addressing current safeguarding challenges.

Specialised Role Requirements

Staff members with specific responsibilities within the Esports programme receive additional targeted training relevant to their roles. This includes enhanced technical security training for those managing gaming platforms and advanced mental health support training for staff overseeing competitive events.

Review and Adaptation

The training programme undergoes annual review to ensure it continues to meet the evolving needs of our Esports provision. This review process incorporates feedback from staff, pupils, and parents, alongside analysis of emerging safeguarding challenges in the digital gaming environment. Regular updates ensure our training remains at the forefront of educational safeguarding practice.

SAFEGUARDING IN ESPORTS EDUCATION

Through this comprehensive approach to professional development, we ensure that all staff members possess the necessary skills and knowledge to maintain the highest standards of pupil safety within our Esports provision. This commitment to continuous learning and development underpins our ability to provide a secure and enriching educational experience in the dynamic field of Esports.

These educational opportunities are delivered within our comprehensive safeguarding framework, ensuring that all activities maintain appropriate protections for our pupils. Staff receive specific training in identifying and managing risks associated with Esports education, while supporting pupils in exploring these emerging career pathways safely.

Esports-Designated Safeguarding Lead Responsibilities

The Esports-Designated Safeguarding Lead serves as the primary authority for ensuring pupil safety within our Esports provision. This specialist role operates in conjunction with the school's broader safeguarding framework while addressing the unique challenges presented by digital gaming environments and competitive Esports activities.

Strategic Oversight and Policy Development: The Designated Lead maintains primary responsibility for developing and implementing comprehensive safeguarding protocols specific to Esports education. This encompasses the creation and regular review of risk assessment frameworks, the establishment of clear reporting procedures, and the development of responsive intervention strategies. Working closely with senior leadership, the Lead ensures that Esports safeguarding measures align with both statutory requirements and emerging best practices in digital safety.

The role requires continuous evaluation of our safeguarding framework, incorporating new protective measures as the Esports landscape evolves. This includes regular consultation with external safeguarding bodies, gaming industry safety specialists, and educational authorities to maintain exemplary standards of pupil protection.

Operational Management and Risk Assessment: Daily operational oversight forms a core component of the Lead's responsibilities. This includes conducting thorough safety assessments of all digital learning environments, verifying the security of gaming platforms, and ensuring appropriate monitoring systems remain active and effective. The Lead maintains comprehensive documentation of all safety measures and regularly reviews their effectiveness through systematic audit procedures.

Through close collaboration with technical staff, the Lead ensures that all gaming environments maintain appropriate security configurations and content filtering systems. This includes regular testing of safety protocols and swift implementation of necessary security updates or enhancements.

Communication and Stakeholder Engagement: The Designated Lead serves as the primary point of contact for all Esports safeguarding matters, maintaining clear communication channels with pupils, parents, staff, and external agencies. This role involves developing comprehensive communication strategies that ensure all stakeholders remain informed about safety measures and procedures.

Parent engagement represents a particular focus, with the Lead ensuring that families receive regular updates about safety protocols, gaming guidelines, and support resources. This includes facilitating parent information sessions and providing guidance on supporting safe gaming practices at home.

Incident Response and Management: When safeguarding concerns arise, the Designated Lead coordinates all response activities, ensuring swift and appropriate action to protect pupil wellbeing.

SAFEGUARDING IN ESPORTS EDUCATION

This includes implementing established response protocols, coordinating with relevant staff members, and maintaining detailed incident documentation.

The role requires careful assessment of each situation to determine appropriate intervention levels and necessary escalation pathways. Working within established frameworks, the Lead ensures that serious concerns receive immediate attention and that all statutory reporting requirements are met promptly and comprehensively.

Professional Development Coordination: The Designated Lead plays a central role in maintaining staff expertise in Esports safeguarding. This includes identifying training needs, coordinating professional development activities, and ensuring all staff maintain current safeguarding certifications. The Lead also provides specialist guidance to staff members regarding specific safeguarding challenges within the Esports environment.

External Partnerships and Compliance: Maintaining effective relationships with external organisations forms an essential aspect of the role. The Designated Lead serves as the primary liaison with local safeguarding authorities, gaming industry safety teams, and educational bodies. This includes regular participation in professional networks and ensuring our safeguarding measures align with evolving regulatory requirements.

The Lead maintains responsibility for ensuring compliance with all relevant legislation and educational guidelines, adapting our safeguarding framework as necessary to meet changing requirements. This includes regular review of our practices against statutory frameworks and implementation of necessary updates to maintain exemplary standards of pupil protection.

Through these comprehensive responsibilities, the Esports-Designated Safeguarding Lead ensures the maintenance of a secure and supportive environment for all pupils engaging in our Esports provision. This role represents our commitment to maintaining the highest standards of safety and wellbeing within our innovative educational programme.

These educational opportunities are delivered within our comprehensive safeguarding framework, ensuring that all activities maintain appropriate protections for our pupils. Staff receive specific training in identifying and managing risks associated with Esports education, while supporting pupils in exploring these emerging career pathways safely.

References/Links to Statutory and Guidance Documents

Keeping Children Safe in Education (2026): [Keeping Children Safe in Education \(2026\)](#)

Department for Education – Working Together to Safeguard Children 2026: [Working Together to Safeguard Children 2026](#)

Filtering and Monitoring Standards for Schools and Colleges (2022), (Updated 2026): [Filtering and Monitoring Standards for Schools and Colleges \(2022\), \(Updated 2026\)](#)

UKCIS – [Sharing Nudes and Semi-Nudes: Advice for Education Settings Working with Children and Young People \(2024\)](#)

Generative AI: Product Safety Standards (2026) [Generative AI: Product Safety Standards \(2026\)](#)

UKCIS – [Education for a Connected World](#)

DfE: [Safeguarding and Remote Education](#)

SAFEGUARDING IN ESPORTS EDUCATION

DfE Guidance: [Remote education](#)

SHS Preventing Extremism and Radicalisation Policy (2026-2027) [SHS Preventing Extremism and Radicalisation Policy \(2026-2027\)](#)

SHS Safeguarding and Child Protection Policy (2026-2027) [SHS Safeguarding and Child Protection Policy \(2026-2027\)](#)

SHS Digital Safety Agreement Policy (2026-2027) [SHS Digital Safety Agreement Policy \(2026-2027\)](#)

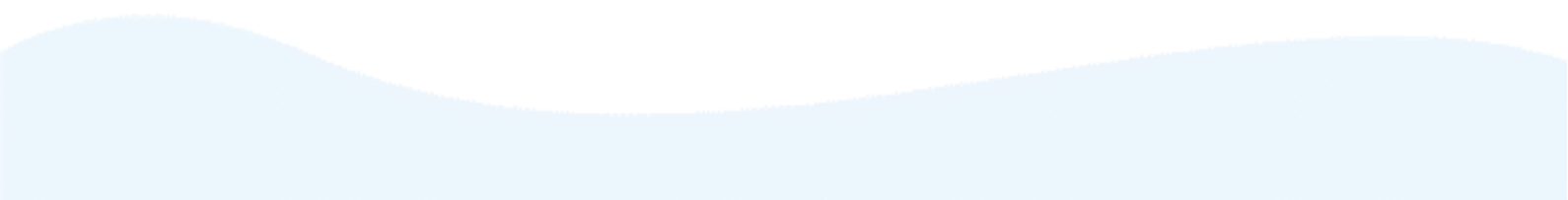
Ann Craft Trust: [Safeguarding in Esports](#)

Brabners: [Esports Safeguarding](#)

NSPCC: [Keeping Children Safe Online](#)

NSPCC: [Social Media, Online Communities and Safeguarding](#)

OFCOM Report: [Children and Parents - 2025 Media use and attitudes](#)



Appendix 1: Risk Assessing Esports Education – 2026-2027

[SHS Esports Education Risk Assessment 2026-2027.docx](#)

Appendix 2: Risk Assessing Esports Competitions – 2026-2027



Esports Competitions – Risk Assessment 2026-2027

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

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

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	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	Teacher

SAFEGUARDING IN ESPORTS EDUCATION



		safeguarding concern. AI-generated or manipulated images, virtual backgrounds or video may be used to impersonate others or conceal safeguarding concerns.			environments. - Manage call, and call immediately for all if high risk is exposed. - Report concerns immediately, following Safeguarding policy. Staff should remain professionally curious regarding changes in learners' appearance, behaviour and home environment. AI-generated imagery or impersonation should be reported immediately to the Designated Safeguarding Lead (DSL).	
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 space for monitoring. Students must not record, livestream or share images from lessons.	Teacher / Education Team



					Personal messaging platforms (e.g. Discord, WhatsApp, Snapchat) must not be used to communicate with competitors unless authorised through the school. Staff supervise all online interactions throughout competitions.	
Online Recordings	Screenshot or screen recording of children and staff from virtual lessons being misused	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. Screenshots, recordings, AI manipulation or redistribution of images may be used for cyberbullying, harassment, impersonation or other safeguarding concerns.	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. AI-generated manipulation of images treated as a safeguarding concern. Concerns reported to DSL and recorded in Athena.	Teacher / Education Team
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

SAFEGUARDING IN ESPORTS EDUCATION



Security	Pupils password use this can be shared by the pupil at home	Shared passwords or reset passwords can mean that students and others could misuse the system. Danger of non-authorized access to restricted or secure areas. Phishing Compromised accounts Malware Credential theft Unauthorized access	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. - Strong passwords - Multi-factor authentication where available - Staff awareness of phishing - Report compromised accounts immediately - Only approved software downloaded	Education Team / Teachers / ICT Team
Security	Filtering & Monitoring	Filtering or monitoring systems fail to identify safeguarding concerns during online activity.	M	H	- Filtering and monitoring reviewed regularly. - Staff understand limitations. - Alerts investigated promptly. - Concerns escalated to DSL. - Systems reviewed by IT.	DPO/ 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,	The University of California shows links between blue light exposure and lack of sleep and poor ocular health Prolonged screen use may have adverse effects on wellbeing, sleep and visual comfort. research It can also be a contributing factor to	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	Teacher



	damaging eyesight.	development of various diseases and health conditions. Extended gaming may negatively affect emotional wellbeing, sleep, concentration and mental health.			- can be completed without using a computer or other electronic device to help reduce screen time. - Regular wellbeing check-ins. - Appropriate movement breaks. - Staff monitor signs of distress.	
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, during lessons using their Sophia High School account.	L	H	- PSHE Curriculum (Holistic Horizons), sequenced through year groups will address e-safety as required by <u>DFE</u>. - Appropriate schedule of lessons on e-safety and keeping safe online as recorded on the school calendar, including student and parent workshops. - 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. - Filtering and monitoring systems support safe internet access. - Staff understand filtering limitations. - Concerns escalated to DSL. - Students taught online safety, including AI risks.	Teachers/ Education Team

SAFEGUARDING IN ESPORTS EDUCATION



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 may be approached by unknown users through chat facilities.	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. - Students never share usernames, contact details or social media. - Report any concerning communication immediately. - Teacher supervision maintained.	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. - Attendance expectations for Esports activities are communicated to parents and monitored in accordance with the School Attendance Policy.	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



Other learners	Other learners may use inappropriate language/ distribute offensive messages or unauthorised links. May invite non-authorised others to participate. Other learners must never share personal contact details, social media handles, gaming usernames used outside school, passwords, telephone numbers or location information with participants from other organisations	Whilst we cannot directly control the actions of those from other centres, we can inform our students of the dangers, and why/how to avoid having unnecessary communication and possible antagonising interactions with opponents. This will reduce the likelihood of an incident occurring. Learners will always be supervised by staff from both centres to reduce the likelihood of incidents occurring and prevent them from escalating, should the need arise.	M	M	- Online competitions should have appropriate safeguarding policies and procedures in place when working with minors, meeting <u>DfE guidance</u>. - Teacher to always be present with learners online. - Students are educated regarding what is and is not appropriate and they understand the urgent need to report this when they see it. - Students will understand that they should avoid non-essential communications with the opposing team to minimise risks. - Competition providers should have named safeguarding contacts. - Safeguarding procedures shared before events. - Staff know emergency reporting procedures. - Staff maintain professional curiosity regarding learner interactions.	Teacher / Education Team / Competition Provider / Host
Political/Cultural Conflict	Other learners from other centres may	Whilst we cannot directly control the actions of those from other centres, we can inform our students of the	L	L	- Students are educated regarding what is and is not appropriate and	Teacher / Education Team /

SAFEGUARDING IN ESPORTS EDUCATION



	challenge or disparage a range of alternative cultural and religious beliefs.	dangers, and why/how to avoid having unnecessary communication and possible antagonising interactions with opponents. Other participants are not aware of the importance of cybersecurity and safe/proper internet use. Direct abusive communication (passive-aggressive, profane language, discriminatory statements) are shared either spoken or written in the chat with participants. Other participants are not always supervised by staff at all times. Extremist narratives Hate speech Online radicalisation			they understand the urgent need to report this when they see it. - Teachers from both schools are always present to observe, monitor and prevent. Safeguarding policies should be understood and followed by all. - Digital Agreements signed by all participants to give understanding of expectations and rules to be agreed and followed. - Students clearly informed that they should never exchange personal information. Staff trained in Prevent. Online content escalated where appropriate. Appropriate filtering and monitoring.	Competition Provider / Host
--	---	---	--	--	---	-----------------------------



Digital Content	AI-generated content and impersonation	Learners may encounter or create AI-generated images, videos, voice recordings, avatars or messages which could be misleading, harmful or used for: • impersonation • cyberbullying • deepfakes • sexual harassment • grooming • misinformation	M	M	Safe and ethical AI taught. Staff trained to recognise AI-generated content. AI misuse treated as safeguarding concern. Identity verified where concerns exist. Report to DSL immediately. Parents informed where appropriate. Concerns reported immediately under safeguarding procedures. AI-generated harassment, bullying or impersonation treated as safeguarding concerns.	Teacher / Education Team
Online Communities	Exposure to extremist or harmful ideologies	Learners may encounter extremist, discriminatory or harmful ideological content through gaming communities, voice chat, forums, livestreams or associated online platforms.	L	M	Students are taught to recognise and report concerning content. Staff receive Prevent Duty training. Any concerns are managed in accordance with the School's Safeguarding and Prevent procedures. Teacher supervision is maintained during organised events.	Teacher / Education Team
Data Protection & Privacy	Personal information, gaming identities or recordings may be	Learners may have their personal information, gaming identities, recordings, voice communications or other personal data collected, stored or shared inappropriately through gaming or competition platforms,	M	H	GDPR-compliant platforms. Minimum personal information. First names only. Parent information. DPIA completed where required. Secure storage of recordings.	DPO/Teacher / Education Team

SAFEGUARDING IN ESPORTS EDUCATION



	disclosed inappropriately	resulting in data protection breaches or safeguarding concerns.				
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	- 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

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.

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 EDSL	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 DUA 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	Katie Todd (DSL)
--------------------	------------------