ONLINE SAFETY

V7 OCTOBER 2026

Author	Training and Quality Manager
Review Date	August 2027

Tilford House, Farnham Business Park, Weydon Lane, Farnham GU9 8QT
t. 01252 514999 **e.** info@overworld-amp.uk **w.** www.overworld-amp.uk

Version 2 Nov 24	Filtering and Monitoring Section Expanded. Greater emphasis on chaperoning and supervision in all sessions. Remote Delivery Safeguards Enhanced. Staff responsibilities further detailed e.g. explicit ban on GTA
Version 3 Nov 24	Cyberbullying Policy added (Appendix 2)
Version 4 Aug 25	Legal Framework Added. Updated Definitions and Risks: new references to generative AI, misinformation, and disinformation have been added. Enhanced Filtering and Monitoring Detail. Use of MyConcern for incident reporting now explicitly stated. All staff now receive updated training on emerging online harms and the role of AI. Specified we support young people in digital literacy, critical thinking, and safe engagement with AI-generated content. Appendix 2 - Cyber Bullying updated to reflect a more detailed response procedure and includes relevant legislation for online abuse.
Version 5 Dec 25	Clarification on uploading and public activity.
Version 6 Sep 26	Comprehensive review and restructure. Updated in line with KCSIE 2026. Renamed to Online Safety Policy. Specialist guidance and Acceptable Use Agreement revised.

Contents

1. PURPOSE 3
2. SCOPE 3
2. LEGAL AND STATUTORY FRAMEWORK 3
4. DEFINITIONS 4
5. ROLES AND RESPONSIBILITIES 5
6. ONLINE SAFETY ARRANGEMENTS 6
7. ONLINE SAFETY CONCERNS 9
8. MONITORING AND REVIEW 10
APPENDIX 1 - ACCEPTABLE USE AGREEMENT 11

1. PURPOSE

1.1 Overworld AMP Limited ("the Provision") recognises that digital technology is central to education, communication, creativity and everyday life. Technology, including gaming, streaming and digital content creation, forms an integral part of the Provision's educational and therapeutic approach at Tilford House.

1.2 The Provision is committed to creating a safe online environment where young people can develop digital skills, participate confidently and enjoy the benefits of technology whilst being protected from online harm.

1.3 This policy sets out how the Provision:

- promotes online safety;
- manages online risks;
- protects young people from online harm;
- responds to online safety concerns; and
- fulfils its safeguarding responsibilities in relation to the use of digital technology.

1.4 Online safety is everyone's responsibility and forms part of the Provision's wider safeguarding culture.

2. SCOPE

2.1 This policy applies to:

- all young people attending the Provision;
- all employees, volunteers, agency staff, contractors and visitors;
- all digital devices owned, managed or authorised by the Provision;
- authorised personal devices used for educational purposes;
- all online platforms, software and digital services used by or on behalf of the Provision; and
- activities undertaken on-site, off-site and remotely.

2.2 This policy applies whenever digital technology is used in connection with the Provision, including:

- teaching and learning;
- gaming and esports activities;
- digital content creation;
- livestreaming and broadcasting;
- online communication and collaboration;
- virtual or remote sessions; and
- any other online activity undertaken on behalf of the Provision.

2. LEGAL AND STATUTORY FRAMEWORK

This policy has been developed with regard to relevant legislation and safeguarding guidance, including:

- Keeping Children Safe in Education (2026);
- Working Together to Safeguard Children (2026);
- Online Safety Act 2023;
- Education Act 2002;

- Children Acts 1989 and 2004;
- Counter-Terrorism and Security Act 2015 (Prevent Duty);
- Data Protection Act 2018;
- UK General Data Protection Regulation (UK GDPR);
- Human Rights Act 1998;
- Equality Act 2010;
- Sexual Offences Act 2003;
- Communications Act 2003; and
- Malicious Communications Act 1988.

The Provision also has regard to relevant guidance issued by the Department for Education (DfE), UK Council for Internet Safety (UKCIS), National Crime Agency (CEOP) and the National Cyber Security Centre (NCSC).

4. DEFINITIONS

For the purposes of this policy, online safety refers to the safe, responsible and appropriate use of digital technology, online services and electronic communications to protect young people from harm and promote positive digital experiences.

4.1 **Online Risks** are broad and ever evolving, but can be categorised into four areas of risk:

4.1.2 **Content**

Being exposed to illegal, inappropriate, or harmful content, for example:

- pornography,
- racism,
- misogyny,
- self-harm,
- suicide,
- antisemitism,
- radicalisation,
- extremism,
- extreme sexual or physical violence,
- misinformation, disinformation (including fake news) and conspiracy theories.

4.1.3 **Contact**

Being subjected to harmful online interaction with other users or generative AI applications that simulate this; for example:

- peer-to-peer pressure,
- commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.

4.1.4 **Conduct**

Online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images, including those generated using AI and online bullying.

4.1.5 **Commerce**

Risks such as online gambling, inappropriate advertising, phishing and or financial scams.

4.3 **Generative Artificial Intelligence (AI)**, for the purposes of this policy, means artificial intelligence technology capable of creating new digital content, including text, images, audio, video, code or other

data. Whilst generative AI can support learning and creativity, it may also present safeguarding risks, including through inaccurate or inappropriate content, misinformation, deepfakes, manipulation and the generation of harmful material.

4.4 **Deepfake** means digitally manipulated or artificially generated image, audio or video content which realistically depicts a person, event or activity that did not occur or did not occur as represented. This includes AI-generated or digitally altered nude or semi-nude imagery ('deep nudes').

4.5 **Cyberbullying** means the use of digital technology to threaten, intimidate, harass, humiliate or deliberately target another person.

4.6 **Digital Footprint** means the information and data created or left through an individual's use of digital technologies and online services, including posts, comments, images, videos, searches and other online activity.

4.7 **Filtering** means technical measures used to block or restrict access to harmful or inappropriate online content.

4.8 **Monitoring** means the systems, processes and strategies used to identify potentially harmful or inappropriate online activity and safeguarding concerns.

4.9 **Personal Data** means any information relating to an identified or identifiable living individual. This may include names, contact details, identifiers, online identifiers, photographs, video, location data and other information which identifies an individual directly or indirectly.

4.10 **Online Grooming** is the process by which an individual establishes a relationship with a young person online for the purpose of abuse, exploitation or criminal activity.

4.11 **Sextortion** (including financially motivated sexual extortion) is a form of exploitation in which a person is threatened, blackmailed or coerced following the sharing, or purported sharing, of intimate images or videos. Demands may include money, further images or sexual content, or other actions.

5. ROLES AND RESPONSIBILITIES

5.1 **Directors** are responsible for ensuring that:

- appropriate online safety policies, procedures and technical controls are in place;
- online safety is embedded within the Provision's safeguarding culture;
- appropriate filtering and monitoring systems are implemented and reviewed annually;
- sufficient resources are available to support effective online safety arrangements; and
- staff receive appropriate training and support.

5.2 **Designated Safeguarding Lead (DSL) And Deputy Designated Safeguarding Leads (DDSLS)** are responsible for:

- leading the Provision's response to online safety concerns;
- ensuring online safety incidents are managed in accordance with the *Safeguarding* and *Young Person Protection* Policies;
- making referrals to external agencies where appropriate;
- maintaining accurate safeguarding records on MyConcern;
- supporting staff, young people and families where online safety concerns arise;
- monitoring trends and emerging online risks; and
- ensuring staff receive appropriate online safety training.

5.3 **IT Lead** is responsible for:

- maintaining secure digital infrastructure;
- implementing and maintaining appropriate filtering and monitoring systems;

- managing user accounts and access permissions;
- investigating technical security incidents;
- supporting the DSL where online safety incidents involve technical systems; and
- reporting any identified safeguarding concerns immediately.

5.4 **Staff** are responsible for:

- promoting safe and responsible use of technology;
- maintaining professional boundaries in all online communications;
- supervising young people appropriately during online activities;
- following the Provision's acceptable use requirements;
- remaining alert to signs of online abuse, exploitation or harmful online activity;
- reporting concerns immediately to the DSL or DDSL;
- recording safeguarding concerns on MyConcern;
- completing mandatory online safety and safeguarding training; and
- modelling safe, respectful and responsible online behaviour.

Staff must not:

- communicate with young people using personal accounts or unauthorised platforms;
- share personal contact details;
- access inappropriate online content whilst undertaking their duties; or
- promise confidentiality where an online safety concern is disclosed.

5.5 **Young People** are expected to:

- use technology safely and responsibly;
- understand, complete and follow the *Acceptable Use Agreement*;
- treat others with respect online;
- protect their personal information;
- report anything online that makes them feel unsafe or uncomfortable;
- follow staff instructions when using digital technology; and
- contribute positively to the Provision's online community.

5.6 **Parents and Carers** are encouraged to:

- support safe and responsible use of technology at home;
- help their young person to understand and complete the *Acceptable Use Agreement;*
- work in partnership with the Provision where online safety concerns arise;
- inform the Provision of significant online safety concerns that may affect a young person's wellbeing;
- support the Provision's expectations regarding online behaviour; and
- provide consent where required for digital activities.

6. ONLINE SAFETY ARRANGEMENTS

6.1 GENERAL PRINCIPLES

The Provision recognises that technology presents both opportunities and risks. Online safety is embedded within the Provision's safeguarding culture and forms part of everyday practice.

All online activities will be appropriately planned, supervised and risk assessed where necessary.

6.2 SUPERVISION

Young people will be appropriately supervised whenever accessing digital technology as part of Provision activities.

Staff must:

- supervise young people throughout online activities;
- ensure activities are appropriate to the young person's age, understanding and individual risk assessment;
- remain physically present unless alternative supervision arrangements have been approved;
- intervene where online behaviour becomes unsafe or inappropriate;
- encourage positive digital citizenship.

6.3 FILTERING AND MONITORING

The Provision operates appropriate filtering and monitoring systems to reduce the risk of young people accessing harmful or inappropriate online content.

Filtering and monitoring arrangements are regularly reviewed to ensure they remain effective and proportionate. The Directors will receive assurance that filtering and monitoring arrangements remain effective, proportionate and appropriate to the Provision's safeguarding risks.

Technical controls do not replace active staff supervision.

6.4 ACCEPTABLE USE

Staff and young people are required to follow the Provision's *Acceptable Use Agreement* when using digital technology on behalf of, or whilst participating in activities provided by, the Provision.

The Provision reserves the right to restrict, suspend or remove access to any digital device, platform or online service where its use presents a safeguarding, security or operational risk.

6.5 PERSONAL DEVICES

The Provision recognises that personal digital devices including mobile phones, tablets, gaming consoles, smart watches, VR equipment and other internet-enabled devices, may form part of a young person's educational experience, communication, emotional regulation and independence. Their use is managed through appropriate supervision and safeguarding arrangements.

Young people may, with staff permission and where appropriate:

- use personal mobile phones and wearable technology;
- bring personal gaming consoles or devices into the Provision;
- access their own gaming or online accounts; and
- communicate with friends through approved online platforms where this forms part of supervised activities.

The use of personal devices is subject to appropriate staff supervision and may be restricted where it presents a safeguarding, behavioural or educational concern.

Young people are encouraged to keep personal mobile phones in their bags unless they are being used for an agreed educational, wellbeing or communication purpose.

Where young people access online gaming, virtual reality or voice communication, activities must remain visible or audible to supervising staff.

The expectations for staff using personal devices are detailed within the *Employee Handbook*. Staff must ensure that the use of personal devices never compromises safeguarding arrangements or professional boundaries. In particular, staff must not:

- communicate with young people outside authorised Provision systems;
- use personal devices to take photographs, videos or audio recordings in connection with their work for the Provision;
- record meetings, conversations or other workplace activities unless expressly authorised by the Provision;
- access or store confidential Provision information on personal devices; or
- circumvent the Provision's safeguarding, filtering or monitoring arrangements.

6.6 ARTIFICIAL INTELLIGENCE (AI)

The Provision recognises that artificial intelligence (AI) is becoming an increasingly important part of education, creativity and everyday life. Young people may use AI to support learning, creativity, communication and accessibility where this is educationally appropriate and supervised.

The Provision will support young people to develop the knowledge and critical thinking skills needed to use AI safely, responsibly and ethically.

Staff and young people should remain alert to the safeguarding risks associated with AI, including:

- misinformation and disinformation;
- AI-generated or manipulated images, audio and video (deepfakes);
- online scams and impersonation;
- inappropriate or harmful content;
- the sharing of personal or confidential information; and
- the misuse of AI to harass, bully or exploit others.

Any safeguarding concerns arising from the use of AI will be managed in accordance with the Provision's *Young Person Protection Policy*.

6.7 PHOTOGRAPHY, VIDEO AND DIGITAL MEDIA

The creation and use of photographs, video and other digital media must:

- comply with the Provision's consent procedures (see *Data Protection and GDPR* Policy);
- protect the privacy and dignity of young people;
- avoid unnecessary identification of individuals;
- be stored securely; and
- only be shared where appropriate authorisation has been obtained.

6.8 SPECIALIST ACTIVITIES

The Provision delivers educational activities involving gaming, digital content creation, livestreaming and other online platforms at Tilford House. These activities are subject to additional safeguarding arrangements and must be delivered in accordance with the relevant specialist policies:

- *Gaming;*
- *Digital Content Creation and Online Communication;* and
- *Minecraft Server Moderation*.

6.9 REMOTE DELIVERY

The Provision recognises that some young people may be unable to attend in person due to illness, anxiety, distance or other exceptional circumstances. Where appropriate, educational or mentoring-style sessions may be delivered remotely using approved platforms.

Remote sessions are subject to the same safeguarding expectations as face-to-face provision.

The following safeguards apply:

- sessions must be planned and authorised in advance;
- the date, time, purpose and member of staff delivering the session must be agreed beforehand;
- only approved platforms and Provision accounts must be used;
- access links must be password protected where available and not shared with unauthorised individuals;
- staff must ensure appropriate privacy settings are in place before commencing the session;
- staff must conduct sessions from a professional and appropriate environment;
- cameras, microphones and other platform controls must be managed to maintain a safe learning environment;
- expectations regarding behaviour and participation must be clearly communicated to young people and, where appropriate, parents or carers;
- any safeguarding concerns arising during a session must be managed in accordance with the *Young Person Protection Policy*; and
- all remote sessions conducted by staff based outside of the provision, will be recorded and retained securely for one month. Where a recording forms part of a safeguarding investigation or other formal process, it may be retained for longer in accordance with the Provision's retention arrangements.

Further guidance for staff delivering remote sessions is contained within the *Employee Handbook*.

6.10 SECURITY

The Provision takes appropriate technical and organisational measures to protect its digital systems, networks and information from unauthorised access, misuse and cyber threats.

These arrangements include:

- secure user accounts and password management;
- filtering and monitoring systems;
- appropriate access controls;
- secure management of Provision-owned devices;
- secure storage of digital information; and
- the reporting and investigation of suspected cyber security incidents.

All staff receive cyber security awareness training, including the National Cyber Security Centre's Cyber Security Training for Schools (or equivalent), and are expected to apply this learning when using the Provision's digital systems.

Staff must also follow the requirements set out in the *Employee Handbook, Data Protection and GDPR Policy*.

7. ONLINE SAFETY CONCERNS

7.1 Online safety concerns may arise through the use of digital technology both within and outside the Provision. Concerns may come to light through:

- observations made by staff;
- disclosures from young people;
- reports from parents, carers or partner agencies;

- filtering or monitoring systems;
- online activities undertaken as part of the Provision's educational offer; or
- concerns identified whilst delivering remote sessions.

7.2 Online safety concerns may include, but are not limited to:

- cyberbullying;
- online grooming;
- child sexual abuse or exploitation;
- criminal exploitation;
- radicalisation;
- sextortion;
- sharing or requesting nude or semi-nude images;
- exposure to harmful, illegal or inappropriate content;
- online harassment or hate incidents;
- misuse of artificial intelligence;
- online scams or fraud;
- identity theft or impersonation; and
- any other online activity that places a young person or another person at risk of harm.

7.3 All online safety concerns must be reported and managed in accordance with the *Young Person Protection Policy*. Incidents involving the sharing of nude or semi-nude images will be managed with regard to current UKCIS guidance for education settings working with young people.

Where an online safety concern also constitutes bullying, it will additionally be managed in accordance with the *Tackling Bullying* and *Positive Interactions* Policies.

Where a concern involves the misuse of technology, the Provision may temporarily restrict access to devices, accounts or online services whilst the matter is assessed.

8. MONITORING AND REVIEW

This policy will be reviewed annually, or sooner where required, to reflect changes in legislation, statutory guidance, technology, safeguarding practice or the Provision's operational arrangements.

The effectiveness of this policy will be monitored through quality assurance activities, incident reviews, staff feedback, training, and changes in statutory guidance.

APPENDIX 1 - ACCEPTABLE USE AGREEMENT

At Overworld AMP, we use technology, gaming and online platforms to support learning, creativity and wellbeing. I understand that using technology safely is part of helping to keep myself and others safe.

I agree that I will:

- treat other people with kindness and respect when communicating online;
- keep my personal information private and avoid sharing my phone number, home address, social media accounts, photographs or other personal information with people I do not know and trust;
- think carefully about who can see my online profiles and use privacy settings, such as friend lists, where they are available;
- be cautious when using private messaging and only communicate with people I know and trust;
- use strong, unique passwords for my online accounts and change them if I think someone else knows them;
- know how to block, mute or report people who make me feel uncomfortable, worried or unsafe;
- save messages, screenshots or chat logs where it is safe to do so, so that staff or a trusted adult can help if something goes wrong;
- tell a member of staff as soon as possible if anything online worries me or makes me feel unsafe;
- log out of shared devices when I have finished using them;
- never share or request inappropriate photographs or videos, and remember that images shared online can quickly spread beyond my control;
- never arrange to meet someone I have only met online without first speaking to my parent/carer and taking a trusted adult with me;
- use games, websites, apps and online platforms responsibly;
- follow staff instructions when using mobile phones, gaming consoles, virtual reality equipment or other digital devices;
- only livestream, upload or share content where this has been agreed with staff;
- respect other people's privacy and ask permission before taking or sharing photographs, videos or recordings;
- use artificial intelligence (AI) responsibly and never use it to bully, impersonate or harm another person; and
- understand that whilst attending Overworld AMP, I will only be able to access games and online content that staff consider appropriate and safe.

I understand that:

- staff will supervise my online activity whilst I am attending the Provision to help keep everyone safe;
- staff may ask me to stop using a device, game, website, app or online service if they believe it presents a safeguarding, behavioural or wellbeing risk; and
- if I am unsure whether something is safe to do online, I can always ask a member of staff for help.

Young Person's Name _____

Young Person's Signature _____

Parent/Carer Name _____

Parent/Carer Signature _____

Date _____