OVERWORLD

E-SAFETY POLICY & PROCEDURES

NOVEMBER 2023

7 Doman Road, Camberley, Surrey. GU15 3DN
t. 01252 514999 **e.** info@overworld-amp.uk **w.** www.overworld-amp.uk

Contents

INTRODUCTION

The Organisation recognises the benefits & opportunities which new technologies offers to learning. We extensively use technology particularly gaming, streaming & video creation as part of creating a caring, calm, & therapeutic environment in which children & young people (CYP) can thrive. We encourage the use of technology to enhance skills, promote achievement & enable lifelong learning.

The accessibility & global nature of the internet & different technologies mean that we are also aware of potential risks & challenges associated with such use. Our approach is to implement appropriate safeguards within the Organisation while supporting staff, CYP to identify & manage risks independently & with confidence. We believe this can be achieved through a combination of security measures, training, guidance, & implementation of our policies. To further our duty to safeguard CYP & protect them from the risk posed by extremism & radicalisation, we will do all that we can to make our learners & staff stay safe online & to satisfy our wider duty of care.

SCOPE

This policy applies to all CYP & staff & all those who have access to the organisations IT systems, both on the premises & remotely.

All use of the internet & forms of electronic communication such as email, mobile phones, social media, instant messaging, online seminar & video conferencing etc

PURPOSE

- ✓ Ensure the safety & wellbeing of CYP is paramount when anyone is using the internet, social media, or mobile devices
- ✓ Provide staff & volunteers with the overarching principles that guide our approach to online safety
- ✓ Ensure that, as an organisation, we operate in line with our values & within the law in terms of how we use online devices
- ✓ To comply with Keeping Children Safe in Education part 1 & all other legislation, statutory guidance & local policy

DEFINITION

The term e-safety is defined for the purposes of this document as the process of limiting the risks to children & vulnerable adults when using Internet, Digital & Mobile Technologies (IDMTs), through a combined approach to policies & procedures, infrastructures & education, including training, underpinned by standards & inspection.

E-safety risks can be summarised under the following three headings:

Content

- Exposure to age-inappropriate material.
- Exposure to inaccurate or misleading information.

- Exposure to socially unacceptable material, such as that inciting violence, hate or intolerance, sites promoting radicalisation or pornography.
- Exposure to illegal material, such as images of child abuse.
- Illegal downloading of copyrighted materials e.g., music & films.

Contact

- Grooming using communication technologies, potentially leading to sexual assault, CYP sexual exploitation & radicalisation.
- The use of assumed identities on gaming platforms.
- Bullying via websites, mobile phones, or other forms of communication devices. Spyware, e.g., use of Remote Access Trojans/Tools to access private information or spy on their victim.

Commerce

- Exposure of minors to inappropriate commercial advertising.
- Exposure to online gambling services.
- Commercial & financial scams.

FILTERING AND MONITORING

These are often grouped as the same thing however they're two separate yet complementary services. Monitoring relates to the review of user activity on a Network to promote the safeguarding of your CYP and staff.

Keeping Children Safe in Education Guidance suggests finding what is 'appropriate' for the education establishment. This can be a software that monitors everything & sends the data to be reviewed, a managed service that flags & alerts key personnel to specific concerns or it could be a person physically watching CYP during sessions. In the case of Overworld AMP Ltd, CYP are always chaperoned by a member of staff & we require everyone to read & understand then sign to confirm that they will adhere to our E-Safety guidelines (appendix 1).

RESPONSIBILITIES

The reporting responsibilities for e-safety follow the same lines of responsibility as the reporting all other safeguarding concerns or incidents.

All Staff

- Sign & keep to the E-Safety guidelines, Acceptable Use (refer to Appendix 1) at all times
- Responsible for ensuring the safety of CYP & their use of IT while in the care of Overworld, this includes not accessing content that has a rating higher than the age of the CYP without the consent of the parent
- MUST report any concerns or disclosures immediately to Mark Pickering (Designated Safeguarding Lead) mark.pickering@overworld-amp.uk or Steve Mitchell (Deputy Designated Safeguarding Lead) steve.mitchell@overworld-amp.uk or the duty manager if not available

  - NEVER offer assurance of confidentiality everything discussed MUST be reported
- Attend staff training on e-safety & always display a model example to CYP
- Actively promote through embedded good e-safety practice
- Always communicate with CYP people professionally & in line with the *Staff Code of Conduct*

CYP

- Read, understand & sign to confirm they will adhere to the E-Safety guidelines, Acceptable Use
- Receive appropriate e-safety guidance during all supervised sessions
- Inform a member of staff where they are worried or concerned an e-safety incident has taken place involving them or another member of the Organisation
- CYP must always act safely & responsibly when using the internet &/or other media capable technologies

Safeguarding Leads

- Follow the safeguarding reporting procedures
- When necessary, refer to appropriate additional support from external agencies
- Calling e-safety meetings when required
- Ensuring delivery of staff development & training
- Recording incidents
- Liaising with the local authority & external agencies to promote e-safety within the Organisation
- Report to IT Lead any suspected/known breaches & follow up until resolution

IT Lead person

- Ensure that the IT infrastructure is secure & meets best practice recommendations
- IT security incidents are recorded, investigated, & resolved within reasonable a reasonable timescale
- Report any e-safety concerns or disclosures immediately to Designated Safeguarding Lead (DSL)

SECURITY

The Organisation will do all that it can to make sure the network is safe & secure. Every effort will be made to keep security software up to date. Appropriate security measures will include the use of enhanced filtering & protection of firewalls, servers, routers, workstations to prevent accidental or malicious access of systems & information. Digital communications, streaming, posting on YouTube, including email & internet postings, over the Organisation's network, will be monitored in line with the Appendix 1.

The Organisation will comply with guidelines set out by the Counter Terrorism Internet Referral Unit (CTIRU) & has a statutory duty to ensure their systems cannot be used to access any of the websites on the CTIRU list.

Staff are aware of their responsibility of the Prevent Duty & Safeguarding of children & adults at risk. The following guidance must be adhered by all staff communicating online:

- Staff must not post any personal views, beliefs, or opinions
- Staff must challenge any personal views, beliefs or opinions posted by CYP or others relating to the work setting
- Any post considered to isolate or put a CYP at risk should be referred to a Safeguarding Team for further investigation
- Any post considered to promote extreme views should be referred to the Safeguarding Team for further investigation

BEHAVIOUR

The Organisation will ensure that all users of technologies adhere to the standard of behaviour as set out in Appendix 1. The Organisation will not tolerate any abuse of IT systems. Whether offline or online, communications by staff & students should be always courteous & respectful. Any reported incident of bullying or harassment or other unacceptable conduct will be treated seriously, & appropriate action taken.

CYBER BULLYING

Cyber bullying is a form of bullying. As it takes place online, it can happen at any time. Cyber bullies can communicate their messages to a wide audience with speed & often remain anonymous or unidentifiable. Cyber bullying includes bullying via:

- Text message & messaging apps e.g., sending unwelcome texts or messages that are threatening or cause discomfort.
- Picture/video-clips e.g., using mobile device cameras to bully someone, with images usually sent to other people or websites.
- Phone call e.g., silent calls or abusive messages. The bully often disguises their number.
- Email e.g., emailing upsetting messages, often using a different name for anonymity, or using someone else's name to pin the blame on them.
- Chat room e.g., sending upsetting responses to people when they are in a web-based chat room.
- Instant Messaging (IM) e.g., sending unpleasant messages in real-time conversations on the internet.
- Websites e.g., insulting blogs, personal websites, social networking sites & online personal polling sites.

Where incidents become known & conduct is found to be unacceptable, The Organisation will deal with the matter internally. Where conduct is considered illegal, the matter will be reported to the police

USE OF IMAGES & VIDEO

The use of images, or photographs, is popular in teaching & learning & should be encouraged where there is no breach of copyright or other rights of another person

(e.g., images rights or rights associated with personal data). This will include images downloaded from the internet & those belonging to staff or learners.

All CYP & staff receive training on the risks when taking, downloading, & posting images online & making them available to others. CYP >16 &/or their parent/carer if under 18, must complete & sign the *Appendix 3 - Photography & Videos Consent Form within the Data Protection & GDPR Policy* as part of Overworld AMP Ltd onboarding process.

There are particular risks where personal images of themselves, or others are posted onto social networking sites, for example. All media posts produced by our CYP & posted through the Organisation will have content known by supervising staff which is appropriate & acceptable in line with the acceptable use agreement. For the purposes of live streaming & the use of live commentary here again CYP are directly supervised & are required to operate to agreed parameters of appropriate use, including the use of appropriate language & content.

Staff will provide information to CYP on the appropriate use of images. This includes photographs of other learners & staff as well as using third party images. Our aim is to reinforce good practice as well as offer further information for all users on how to keep their personal information safe.

No image/photograph/video can be copied, downloaded, shared, or distributed online without permission from the owner. Photographs & video of activities at Overworld premises should be considered carefully & have the permission from directors before being published. Approved photographs & video should not include names of individuals without consent.

EDUCATION & TRAINING

With the current unlimited nature of internet access, it is impossible for the Organisation to eliminate all risks for staff & CYP. It is our view therefore, that we should support staff & CYP to stay e-safe through regular training & education. This will provide individuals with skills to be able to identify risks independently & manage them effectively.

CYP will be taught about safe & appropriate electronic communication, including the indelible nature of emails, social media presence, images, & other e-communications. Aspects of e-safety such as cyberbullying, revenge porn, trolling & other harassment will be covered in an age-appropriate way, with emphasis placed on respecting oneself & one's peers, to build confidence & understanding among CYP as they interact with technology.

CYP will be regularly reminded about how to always take care when clicking & to seek help from an adult if they see anything that makes them unhappy or that they are unsure about. These digital literacy skills will be developed in keeping with age & ability, with sessions promoting a responsible attitude towards searching the Internet & the importance of personal security measures such as strong passwords & processes for reporting any concerns.

Staff will take part in mandatory Safeguarding training (which includes e-safety) with updates every 2 years or sooner due to changes to technology & social media use.

VIRTUAL SESSIONS & LIVE STREAMING

The Organisation appreciates that some CYP who wish to access our facilities may be unable to attend in-person, due to distance or due to an elevated level of anxiety & inability to leave their own homes. We provide remote gaming sessions through a secure link that is password protected. These sessions are delivered by a member of the mentoring staff team who adhere to Appendix 1.

Additional safeguards such as:

- All sessions are timetabled & agreed by a line manager prior to commencing
- Time & content are known & agreed by a line manager
- Any concerns arising during the session will be reported & if necessary, the session terminated
- The use neutral or plain backgrounds
- Ensure appropriate privacy settings are in place
- Ensure staff understand & know how to set up & apply controls relating to pupil & student interactions, including microphones & cameras
- Set up sessions with password protection & ensure passwords are kept securely & not shared
- Ensure all staff, CYP & parents/carers have a clear understanding of expectations around behaviour & participation

INCIDENTS & RESPONSE

Where an e-safety incident is reported to staff this matter will be dealt with seriously. They will act immediately to prevent, as far as reasonably possible, any harm or further harm occurring. If a CYP wishes to report an incident, they can do so to their supervising mentor, the duty manager or to the Designated Safeguarding Lead. Where a member of staff wishes to report an incident, they must contact their line manager immediately or when possible, bearing in mind that this may require some urgency.

Following any incident, the Organisation will review what has happened & decide on the most appropriate & proportionate course of action. Sanctions may be put in place; external agencies may be involved, or the matter may be resolved internally depending on the seriousness of the incident.

DATA PROTECTION

Personal data will be recorded, processed, transferred, & made available according to the principles of the General Data Protection Regulation (GDPR), which state that personal data must be:

- Processed lawfully, fairly & in a transparent manner
- Collected for specified, explicit & legitimate purposes
- Adequate, relevant, & limited to what is necessary to fulfil the purposes for which it is processed
- Accurate &, where necessary, kept up to date
- Kept for no longer than is necessary for the purposes for which it is processed

- Processed in a way that ensures it is appropriately secure

Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse;
- Use personal data only on secure password protected computers & other devices, ensuring that they are properly 'logged-off' or 'locked' at the end of any session in which they are using personal data;
- Be fully aware of the risks of transferring data using removable media. When personal data is stored on any portable computer system, USB stick or any other removable media, it must be securely deleted once its use is complete.
- It may sometimes be necessary to send confidential information outside the organisation e.g., as part of a safeguarding investigation. Staff must always consider the security of such information. Certain councils will use encryption services

Appendix 1 – E-Safety Guidelines & Acceptable use form

For Young People

- ✓ Keep your personal information private – avoid sharing personal information such as your phone number, home address, social media tags or photographs with people you do not know in person & trust.
- ✓ Check whether the social media networks you use allow you to create friend lists. These lists let you manage who sees what. For example, you may only want your closest friends to see some information.
- ✓ Use private messages for people you know in person & trust; be careful of private messaging people you do not know.
- ✓ Use a strong & unique password for all your online accounts – a combination of letters, numbers, & symbols (& if you have ever shared it in the past, CHANGE IT).
- ✓ Know how to block someone if they make you feel uncomfortable or upset.
- ✓ Learn how to save chat logs & texts so that if someone does make you uncomfortable or upset, you have evidence to report them.
- ✓ Report any incident to the appropriate member of staff in a timely manner.
- ✓ Remember to log out of a site properly after use, especially on a shared computer.
- ✓ Keep your clothes on when using webcam – images of you could end up in the wrong hands!
- ✓ Think very carefully about meeting someone face to face who you only know online – NEVER do this alone, always talk to your parent/carer before you go ahead with this & take a trusted adult friend along with you.
- ✓ Accept that you will only be able to access age-appropriate games & content, whilst at Overworld sessions

Staff agree to:

- ✓ Only use the organisation's e-mail / Internet / Intranet & any related technologies for professional purposes or for uses deemed 'reasonable'.
- ✓ Comply with the organisation IT security & not disclose any passwords provided to me by the or other related authorities.
- ✓ Ensure that any electronic communications with colleagues, parents & outside agencies are compatible with their professional role.
- ✓ Not give out personal details, such as mobile phone number & personal e-mail address, social media tags to the young people in our care
- ✓ Only use the approved, secure e-mail system(s) for any professional work-related business.
- ✓ Ensure that personal data is kept secure & is used appropriately, whether at the Organisation or taken off the premises or accessed remotely.
    - Personal data can only be taken out of the Organisation or accessed remotely with the agreement of the Mark Pickering, MD

- ✓ Not install any hardware of software without permission of Mark Pickering, MD
- ✓ Not browse, download, upload or distribute any material that could be considered offensive, illegal, or discriminatory.
- ✓ Ensure images of service users &/or staff will only be taken, stored, & used for professional purposes in line with agreed practice & with written consent (*Appendix 3 & 4 - Photography & Videos Consent Forms* within the *Data Protection & GDPR Policy*). Images will not be distributed outside the Organisation network without those permissions.
- ✓ All use of the Internet & other related technologies can be monitored & logged & can be made available, on request, to my Line Manager/Managing Director.
- ✓ Respect copyright & intellectual property rights.
- ✓ Ensure that my online activity, both in & outside the Organisation, will not bring my professional role into disrepute & that I accept the guidelines given regarding social networking sites.
- ✓ I will support & promote the policy & help young people to be safe & responsible in their use of ICT & related technologies. This includes supporting them to only access age-appropriate games & content.

Signed ……

Print name ……...

Date ……

For those CYP who are working online only or cannot sign, a verbal acknowledgment will be recorded by a mentor. Email agreement is also accepted.