ONE WORLD
EDUCATION

One World Education

Online Safeguarding Policy

September 2023

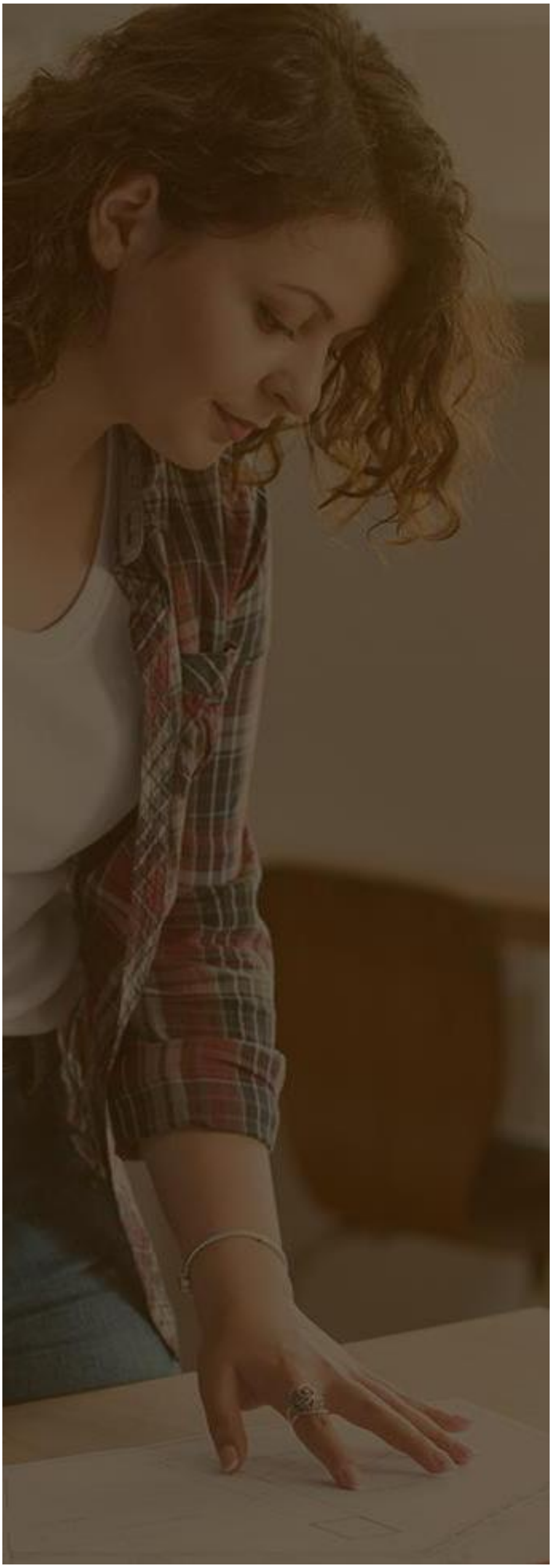

TABLE OF CONTENTS

INTRODUCTION

This policy specifically relates to online outreach and engagement activities. This policy should be read alongside One World Education's Safeguarding Policy.

Legal framework:

This policy has been drawn up on the basis of legislation, policy and guidance that seeks to protect children in England. Summaries of the key legislation and guidance are available on:

- online abuse https://learning.nspcc.org.uk/child-abuse-and-neglect/online-abuse
- bullying https://learning.nspcc.org.uk/child-abuse-and-neglect/bullying
- child protection https://learning.nspcc.org.uk/child-protection-system

Supporting documents

This policy statement should be read alongside our organisational policies, procedures, guidance and other related documents:

- role description for the designated safeguarding officer
- dealing with disclosures and concerns about a child or young person
- managing allegations against staff and volunteers
- recording concerns and information sharing
- child protection records retention and storage
- code of conduct for staff and volunteers
- behaviour codes for children and young people
- photography and sharing images guidance
- safer recruitment
- online safety
- anti-bullying
- managing complaints
- whistleblowing
- health and safety
- induction, training, supervision and support

The purpose of this policy is to:

1.1 Provide specific guidance for all staff that are in contact with One World Education with students whilst interacting or delivering online education to our students.

1.2 One World Education approach to safeguarding students in their care.

This policy applies to all staff involved in the interaction with students and the delivery or supervision of online work and should be read alongside the school's wider Safeguarding policies and practice. This includes School staff members, as well as temporary teachers/tutors/guests/inspectors and visitors that may run workshops from time to time.

One World Education knows that the success of the online safeguarding policy will depend on its effective implementation. It will, therefore, ensure the effective distribution of this Policy with the staff at One World Education along with training around the policy.

One World Education is committed to keeping children safe and ensuring a safe and supportive environment exists for all staff and students engaging in online education provision and engagement activities.

This document is designed to provide One World Education staff working with students online with guidance and a set of procedures to follow to ensure that they adhere to the school's policy on the Safeguarding of Children. This document was written with specific reference to online activities including, but not limited to, interaction on online platforms, instant messaging/chat, live videos/webinars, and mentoring.

Safeguarding concerns in the online education environment can take many forms including, but not limited to, bullying and cyber bullying, peer on peer abuse, youth produced sexual imagery, child sexual exploitation/trafficking, domestic abuse, emotional abuse, grooming, neglect, children missing in education, online abuse, physical abuse, sexual abuse. Abuse could be by adults, or by other children/young people.

We strongly believe that:

- Children and young people should never experience abuse of any kind at any time.
- Children should be able to use the internet for education and personal development, but safeguards need to be in place to ensure they are always kept safe.
- Children should understand how to keep themselves safe when learning online.

We recognise that:

- The online world provides everyone with many opportunities; however, it can also present risks and challenges.
- We have a duty of care to ensure that all children, young people, and adults involved in our organisation are protected from potential harm online.
- We have a responsibility to help keep children and young people safe online, whether they are using our learning environment.
- All children, regardless of age, disability, gender reassignment, race, religion or belief, sex, or sexual orientation, have the right to equal protection from all types of harm or abuse.
- Working in partnership with children, young people, their parents or guardians, health care professionals and agents is essential in promoting young people's welfare and in helping young people to be responsible in their approach to online safety.

1. ONLINE SAFETY

At One World Education it is of up most paramount importance that children are safeguarded from potentially harmful and inappropriate online material. Our School's effective whole school approach to online safety empowers our staff to protect and educate students and staff in their use of technology and establishes devices to identify, intervene in, and escalate any concerns where appropriate.

The scope of issues classified within online safety is considerable, but can be categorised into four areas of risk:

Content:

- Being exposed to illegal, inappropriate or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism.

Contact:

- Being subjected to harmful online interaction with other users; 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.

Conduct:

- Personal online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying.

Commerce:

- Risks such as online gambling, inappropriate advertising, phishing and or financial scams. If you feel your child, students or staff are at risk, please report it to the Anti-Phishing Working Group (https://apwg.org/).

At One World Education, we ensure online safety is at the forefront of our planning and is the occurring and running theme whilst devising and implementing policies and procedures. We consider how online safety is reflected in our unique online learning environment as required in all relevant policies and consider online safety whilst planning the curriculum, any teacher training, the role and responsibilities of the designated safeguarding lead and any parental engagement.

Our Online Safety Policies and Procedures are reflected in our child protection policy. This involves how we approach remote learning in our online learning environment.

2. REMOTE LEARNING

Where children are being asked to learn online at home the Department for Education has provided advice to support schools and colleges do so safely: safeguarding in schools colleges and other providers and safeguarding and remote education. The NSPCC and PSHE Association also provide helpful advice:

- NSPCC Learning - Undertaking remote teaching safely during school closures
- PSHE - PSHE Association coronavirus hub

2.1 **Filters and monitoring**

Whilst considering our responsibility to safeguard and promote the welfare of children and provide our students with a safe environment in which to learn, our education team and proprietors are doing all that we reasonably can to limit children's exposure to risks outlined in our remote learning risk assessment from the school's Digital Education Platform.

As part of this process, we ensure our school has appropriate cyber security and monitoring systems in place through Microsoft for Education. We consider the age range of our children, the number of children, how often they access the system and the proportionality of costs vs risks.

The appropriateness of any filters and monitoring systems are a matter for One World Education and are informed in part by the risk assessment required by the Prevent Duty.

The UK Safer Internet Centre has published guidance as to what "appropriate" filtering and monitoring might look like:

UK Safer Internet Centre: https://saferinternet.org.uk/guide-and-resource/teachers-and-school-staff/appropriate-filtering-and-monitoring

The Prevent duty:
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/439598/prevent-duty-departmental-advice-v6.pdf

2.1 Online Safety & Safeguarding at One World Education School

We will seek to keep children and young people safe by:

- Providing an especially safe online platform for the delivery of our online curriculum through a partnership with Microsoft for Education.
- Microsoft Teams is secure and accessible only by enrolled students, their parents and school staff. All online students, and Early Years parents, will sign to agree and uphold the acceptable use policy and receive instruction in good digital citizenship and Internet safety.
- All One World Education staff have an enhanced DBS check and are carefully screened and specially trained to ensure a positive school environment for everyone.

- Ensuring that appropriate cyber security controls and measures are in place in order to reduce the risk of cyber-attacks which may include **phishing** emails, **malware** from bogus websites and downloads, **ransomware** attacks and **Denial of Service attacks**.

- All members of the Senior Leadership Team have been trained in safer recruitment, to protect students and our school.

In our online school we:

✓ Provide clear and specific directions to staff on how to behave online through our Code of Conduct and **Staying Safe Online** document.

✓ Support and encourage the young people studying with us to use the internet, social media, mobile phones, gaming platforms and any other forms of interactive technology in a way that keeps them safe and shows respect for others through Netiquette.

✓ Ensure all students sign a Correct Use of ICT agreement. All online students sign and pledge to uphold the acceptable use policy and receive instruction in good digital citizenship and Internet safety and Staying Safe Online documents. This also applies to all parents who support and participate in their child's online education.

✓ Support and encourage parents, guardians, Health Care Workers, and agents to do what they can to keep children safe online.

✓ Develop clear and robust procedures to enable us to respond appropriately to any incidents of inappropriate online behaviour, whether by an adult or a child/young person.

✓ Review and update the security of our information systems regularly.

✓ Ensure that usernames, logins, email accounts and passwords are used effectively.

✓ Ensure personal information about the adults and children who are involved in our organisation is held securely and shared only as appropriate.

✓ Ensure that images of children and young people are used only after their written permission has been obtained, and only for the purpose for which consent has been given.

✓ Provide supervision, support and training for staff and any individual involved with One World Education's online activities about online safety.

✓ Examine and risk assess any social media platforms and new technologies before they are used within the school.

3. AREAS OF RISK

3.1 Risk Assessment

Some key risks in online activities are highlighted below. For all new activities planned, a risk assessment will be undertaken which will be approved by the responsible teacher. The activity and risk assessment is then reviewed by the Senior Leadership Team. After this the risk Assessment is then shared with all members of staff on share point.

3.2 IT Safety and Data Protection (additional requirements White Paper 2019)

The below considerations are highlighted in line with the IT safety and data protection White Paper 2019

3.2.1 A Privacy notice is provided on the school website and is easily accessible and provided in language that the participants can understand and are thus fairly informed.

3.2.2 Data protection best practice for any data gathered and stored should be considered in advance of the activity. Data protection should be considered at all stages of design ensuring the approach mitigates the risk to individual participants' information.

3.2.3 The appropriateness of the platform and how they store, process and use personal data should be considered in deciding on an appropriate platform for the delivery of any online lesson/activity.

3.2.4 For assistance in compliance with Data Protection Regulations, please contact the Data Protection Officer at One World Education.

3.3 Social Media

3.3.1 Staff must not engage or communicate with children or children's families via personal or non-school-authorised accounts – all communications should come from an official One-World Education email account.

3.3.2 For all online activities, consent should be sought from parents/carers and the child/young person before posting any identifiable information and/or images of children and young people on official One World Education social media. Teachers should not use any image of students on their personal social media accounts, as this is a breach of the Safeguarding Policy and may be subject to legal action.

3.3.3 Concerns about social media content or posts involving children and young people such as cyberbullying, self-harm, abuse or exploitations should be raised with the designated safeguarding officer in line with the process in the overarching safeguarding policy.

3.3.4 Staff and Students working on online educational provision should abide by the general principles of the code of conduct policy, communications policy, and other relevant One World Education School staff policies.

3.3.5 Staff and students working in our online education environment should not use social media in a way which would breach other school policies, including the safeguarding policy.

3.4 Online Learning and Real Time Interactive Lessons

The measures below are as much about protecting One World Education staff as they are about supporting the students engaging in these lessons/activities.

At One World Education we provide a full-time education following the UK National Curriculum, Australian curriculum or USA curriculum through a blended learning programme which combines live interactive lessons with independent home learning.

Lessons are live streamed using Microsoft teams classroom. Teachers have full control over interactive learning tools including the recording of each lesson for safeguarding purposes. Throughout our programme, students are taught how to use online learning tools safely and our programme is structured to build a sense of community/belonging amongst our student groups. Please read our Microsoft Teams Policy for further details.

3.4.1 Where live streaming is deemed the One World Education has chosen Microsoft Teams as the best platform for delivery of lessons/activities. A risk assessment has been carried out by the Senior Leadership Team and is shared with all the teachers.

3.4.2 Any online activities should only be delivered via online platforms approved for use by One World Education.

3.4.3 Access to the individual platform should only be enabled for the intended participants and is controlled by the Administrative Team.

3.4.4 The platform enables the presenter to control microphones/cameras for participants.

3.4.5 Personal accounts for platforms are not to be used to engage with young people, all activities are organised through Microsoft Teams.

3.4.7 Personal information (including names, contact details and email addresses) should only be accessible to those with the right permissions and should not be publicly viewable.

3.4.8 Staff must never give out personal details to participants such as personal email addresses, personal phone number or social media accounts.

3.4.9 Staff facilitating activities and monitoring any enabled chat should be able to remove students from the platform if necessary.

3.4.10 For all live activities, staff members record sessions and have all undergone the full safer recruitment in education checks. The school admin team is able to monitor messages sent on the chat platform and has access to all recorded lessons, which are reviewed. Live lesson recordings are posted daily to individuals on their assessment page for access by students and families so that learning is visible.

3.4.11 During a live session, staff or students organising it should:

- Ensure that the session is taking place in a neutral area where nothing personal can be seen and there is nothing inappropriate in the background.

- Monitor interactions (verbal and in live chats) to check it is appropriate and relevant, and to deal with any sudden changes or upsetting developments.

3.4.12 If a staff member leaves the session for any reason or has issues accessing Microsoft Teams (e.g. connection issues), they should get in contact with the Senior Leadership Team as soon as possible (by phone if necessary) and attempt to re-join the session if possible. If it is not possible to have a staff member present, then the event should be ended as soon as reasonably possible and this should be communicated to all participants.

3.4.13 At the start, the main speaker should remind participants how to keep themselves safe (as outlined above) in addition to reminding them of the ground rules. This is also a good time to restate any pre-shared privacy notice to participants and particularly important if participants can override any central setting and share their own video unless asked by the teacher.

3.4.14 If staff share their screens at any point they must ensure that there is nothing inappropriate on the screens/internet pages/browser history.

3.4.15 Challenging behaviour or inappropriate comments should be dealt with immediately, which may involve muting or removing the offender from the platform in line with the school Behaviour and Exclusion Policies.

3.4.16 You should also ensure that the participants:

- Do not share private information about themselves.
- Do not respond to contact requests from people they do not know.
- Understand who they should contact if they hear anything upsetting or inappropriate.

3.4.17 For any interactive live streaming, consent is sought and recorded from parents/guardians of any under-18 participants.

3.4.18 A signed Digital Safety Agreement and code of conduct should be received from all participants which should include the consequences in the case of inappropriate behaviour.

3.4.19 At the start of a session participants should be reminded of this code of conduct, not to take photographs of the screens or share any images, and how they can report any concerns.

3.4.20 If a safeguarding disclosure is made by a participant, the School’s Safeguarding Policy should be followed.

3.4.21 Staff should not be in a private chat/video call 1-2-1 with a participant, without the session recording or a parent of the student present. If this happens by accident (someone else loses signal etc.) they should immediately come out of the breakout room/chat/end the session.

3.4.22 A member of the Senior Leadership Team will be in all the Microsoft Teams pages and will have access to all the students’ learning resources.

4. ENHANCED DISCLOURSE AND BARRING (DBS)

DBS checks are required for all staff involved in online delivery; the requirements for this are outlined in our School’s Safer Recruitment Policy.

Records of pre-employment checks and subsequent training are held by the Director of Education in the School’s Single Central Register.

5. KEY CONTACTS

For further information or any questions, you may have relating to One World Education Online Safety Policy please contact Chenaie Roberts via email on ceo@one-worldeducation.com.

Written by:	Chenaie Roberts
Date:	01/04/2023
Implementation date:	01/09/2023
Review date:	March 2024