

E-safeguarding policy

April 2025

Meeting Prevent duties		
No	Policy Item	Involving
1	<p>Statement</p> <p>This policy, adapted from NSPCC Learning, should be read alongside CIE Oxford policies and procedures on child protection and safeguarding.</p> <p>CIE Oxford and its staff (including Host families) will do as much as possible to keep children and young people safe. The needs of the child are paramount and procedures that are in place should relate to all aspects of the child's life whether that applies to the school setting, the social enrichment programme or the place the child is living. CIE Oxford accepts responsibility for ensuring that the various aspects of this guidance are both in place and monitored regularly.</p>	Everyone
2	<p>Aims</p> <ul style="list-style-type: none"> To protect all children and young people attending CIE Oxford and who make use of technology (such as mobiles phones, computers, laptops and the internet) whilst they're within the care of CIE Oxford To provide staff with policy and procedure information regarding e-safety To ensure CIE Oxford is operating in line with its values and within the law regarding how the organisation uses information technology. 	Everyone
	<p>We recognise that:</p> <ul style="list-style-type: none"> The online world provides everyone with many opportunities; however, it can also present risks and challenges 	Everyone

	<ul style="list-style-type: none"> • We have a duty 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 or not they are using CIE's network and devices • 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, carers and other agencies is essential in promoting young people's welfare and in helping young people to be responsible in their approach to online safety. 	
	<p>We will seek to keep children and young people safe by:</p> <ul style="list-style-type: none"> • Appointing an online safety coordinator • Providing clear and specific directions to staff and volunteers on how to behave online through our behaviour code for adults (Employee handbook, Prevent Policy, Care of under 18 Policy, Online Under 18s welfare considerations) • Supporting and encouraging the young people using our service to use the internet, social media and mobile phones in a way that keeps them safe and shows respect for others (behavior guidelines in pre-arrival information, first day induction, classroom displays, T&C in Online learning application form, all school projects, 'No phone Wednesdays') • Supporting and encouraging parents and carers to do what they can to keep their children safe online (pre-arrival information, parental consents, parental locks) • Developing an online safety agreement for use with young people and their parents/carers • Developing 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 (disciplinary procedures in pre-arrival information, Employee handbook, Policies and procedures on CIE Website) • Reviewing and updating the security of our information systems regularly ensuring that usernames, logins, email accounts and passwords are used effectively (in consultation with our IT support) • Ensuring personal information about the adults and children who are involved in our organisation is held securely and shared only as appropriate (GDPR policy, Website Privacy Policy) 	Online safety coordinator/ staff/ parents/ guardians

	<ul style="list-style-type: none"> • Ensuring that images of children, young people and families are used only after their written permission has been obtained, and only for the purpose for which consent has been given (Request for consent in Enrolment form) • Providing supervision, support and training for staff and volunteers about online safety (E-safety training on SSS Learning, Employee handbook) • Provide advice on using social media and live streaming (Online Under 18s welfare considerations; Using Zoom considerations; Social media and online safety guidance) • Examining and risk assessing any social media platforms and new technologies before they are used within the organisation (i.e. Edmodo and Zoom policies). 	
	<p>If online abuse occurs, we will respond to it by:</p> <ul style="list-style-type: none"> • Having clear and robust safeguarding procedures in place for responding to abuse, including online abuse (Child protection/ Safeguarding policy/ Care of under 18s) • Providing support and training for all staff and volunteers on dealing with all forms of abuse, including bullying/cyberbullying, emotional abuse, sexting, sexual abuse and sexual exploitation (SSS Learning or OSCB, Employee handbook, Staff insets) • Making sure our response takes the needs of the person experiencing abuse, any bystanders and our organisation as a whole into account • Reviewing the plan developed to address online abuse at regular intervals, in order to ensure that any problems have been resolved in the long term. 	Students/ staff
	<p>Related policies and procedures</p> <p>This policy statement should be read alongside our organisational policies and procedures, including:</p> <ul style="list-style-type: none"> • Child protection/ Safeguarding/ Care of under 18s policy • Procedures for responding to concerns about a child or young person's wellbeing • Dealing with allegations of abuse made against a child or young person • Managing allegations against staff and volunteers • Code of conduct for staff and volunteers 	Staff/ parents/ guardians

	<ul style="list-style-type: none"> • Anti-bullying policy and procedures (and Cyber-Bullying) • Prevent • Online Under 18s welfare considerations • Photography and image sharing guidance • Social media and online safety guidance 	
	<p>Code of conduct for students</p> <p>Students should follow the guidelines set out in the pre-arrival information and during the induction.</p> <p>The entire main building of CIE is WiFi enabled.</p> <ul style="list-style-type: none"> • Students may use the school's computer equipment to access websites to assist them in their studies, either with or without the guidance of a teacher or the Academic Manager • Students may also use the computers in the common room, or their own devices, to access other websites. <p>However, students should never:</p> <ul style="list-style-type: none"> • Use their mobile phone or any handheld equipment during lessons, meetings or activities, or after lights out (bed time), unless otherwise stated by their teacher in accordance with the Academic Manager • Download any software on CIE devices • Take photographs of others without consent and/ or share them on social media sites • Use school or personal IT/electronic equipment, school WiFi or their own networks to access illegal/inappropriate sites or images in line to Government's PREVENT policy. Such sites include, but are not limited to, those which are racist, sexist, pornographic, homophobic, or are deemed to promote violence or extremist views which contradict core British values. <p>All students must sign the school's e-safety agreement before using any internet enabled device on the school premises. By signing the e-safety agreement students agree to be bound by the agreement.</p>	Students
	<p>Code of conduct for staff</p> <ul style="list-style-type: none"> • Staff should be aware of this policy and behave in accordance with it 	Staff

	<ul style="list-style-type: none"> • Staff should seek the advice of the DSL if they have any concerns about the use of the internet or social media • Staff should communicate any messages they wish to send out to children to the designated staff responsible for the organisation's online presence • Staff should not communicate with children via personal accounts • Staff should not 'friend' or 'follow' children from personal accounts on social media and maintain the same professional boundaries online as they would in person when using organisation accounts • Staff should make sure any content posted on public personal accounts is accurate and appropriate, as children may 'follow' them on social media • Rather than communicating with parents through personal social media accounts, staff should choose a more formal means of communication, such as face-to-face, in an email or in writing, or use an organisational account or website • Staff should avoid communicating with children via email or organisational social media outside of normal office hours • Emails or messages should maintain the organisations tone and be written in a professional manner, e.g. in the same way you would communicate with fellow professionals, avoiding kisses (X's) or using slang or inappropriate language • Staff should not delete any messages or communications sent to or from organisation accounts • Staff should undertake all online safety training offered and gain a basic knowledge of the platforms children use and how to report or remove inappropriate content online • Any concerns reported through social media should be dealt with in the same way as a face-to-face disclosure, according to our reporting procedures • At least one parent must be present during the delivery of any activities via video conferencing platforms at home • Any delivery of activities to children via video conferencing platforms will be supported by an additional member of staff (even if they're not actively delivering) to ensure transparency • Staff and children must not engage in 'sexting' or send pictures to anyone that are obscene 	
3	Contact details	Online Safety

	Online Safety Coordinator Name: Simon Llewellyn Phone/email: 01865 202238/ simon.llewellyn@cie-oxford.com NSPCC Helpline: 0808 800 5000	Coordinator
	We are committed to reviewing our policy and good practice annually or earlier if there are changes in relevant legislation or in response to any significant incidents or changes in circumstances. This policy was last reviewed on: 04/04/2025 Signed: Simon Llewellyn	