CHILD E-SAFETY POLICY

INTRODUCTION

For the purpose of this policy and procedure, the terms 'child' and 'children' refer to anyone up to the age of 18 years (Child Protection Act 1989). The term 'e-safety' is defined as the process of limiting the risks to children when using internet, digital and mobile technologies through a combined approach to policies and procedures, infrastructure, and education.

Action for Conservation ("AFC") is an environmental education charity that runs workshops, residential camps and events for children inside and outside of school environments across the UK. Like most organisations, the internet and digital and mobile technologies play an important role in how we communicate and share information, and we encourage children we work with to use technologies appropriately to share their actions and stay connected. AFC believes that digital technologies can offer children the opportunity to learn and develop, communicate and be creative; however, we understand that children do not always recognise the inherent dangers of the internet and often do not understand that online behaviour can have consequences. Therefore, AFC believes we have a responsibility to understand the dangers that children can face in the online world and ensure we have procedures in place to protect children from these dangers.

SCOPE

This policy applies across our organisation to all staff, trustees, volunteers, children and partner organisations and individuals we work with. AFC's E-Safety Policy will be made available to all partner organisations, volunteers, schools, children and their parents/carers, and staff and used in conjunction with the e-safety policies of partner organisations or schools, where applicable.

LEGAL FRAMEWORK

This policy has been drawn up on the basis of law and guidance that seeks to protect children, namely:

- Children Act 1989
- United Convention of the Rights of the Child 1991
- Data Protection Act 1998
- Sexual Offences Act 2003
- Communications Act 2003
- Malicious Communications Act 1988
- Children Act 2004
- Protection of Freedoms Act 2012
- Equality Act 2010
- Working Together to Safeguard Children Guidance 2013

RELATED POLICIES

This policy should be used in conjunction with other policies that have been developed by AFC, including:

- Child Safeguarding Policy
- Health and Safety Policy
- Our Behaviour and Safety Guidelines for Young People

E-SAFETY RISKS

- Cyberbullying and online abuse.
- Exposure of children to age-inappropriate, socially unacceptable or illegal materials.
- The use of communication technologies to meet and groom children.
- Exposure of children to inappropriate commercial advertising, gambling services and commercial and financial scams.

HOW WE KEEP CHILDREN SAFE ONLINE

- Ensuring that we will, with our partner organisations and schools, promote the e-safety of children as the norm so that it becomes everyone's business.
- Educating all AFC staff and volunteers, partner organisations, children and parents/carers on their rights and responsibilities regarding the safe use of technology and ensuring they have access to this policy.
- Where we encourage the use of technology, ensuring that all children, and where applicable, their parents/carers, are equipped with the knowledge and skill-set to undertake this safely.
- Working to empower all people we work with, including staff, volunteers, partner organisations and individuals, and children to use the internet safely as an essential tool for life-long learning.
- Ensuring that staff, volunteers, partner organisations, children and parents/carers we work with know how to recognise, respond to and report e-safety concerns and access help.
- Helping support parents/carers take a more supportive interest in their child's internet activity.
- Ensuring that all concerns and allegations of abuse will be taken seriously by trustees, staff and volunteers and responded to appropriately - this may require involving parents and children, referral to children's social care services, the independent Local Authority Designated Officer (LADO) for all allegations against staff, trustees and volunteers, and in emergencies, the Police.
- Using this policy in conjunction with AFC's Child Safeguarding Policy.

We are committed to reviewing our policy and good practice annually.

Policy	E-Safety Policy
Review Dates	16/03/2018; 15/03/2019; 11/02/2020; 14/12/2020; 01/04/2022; 19/01/2023; 23/01/2024
Next review due	23/01/2025

E-SAFETY PROCEDURE

DESIGNATED SAFEGUARDING OFFICER (DSO)

Hendrikus van Hensbergen
07766307675
hendrikus@actionforconservation.org

DESIGNATED SAFEGUARDING OFFICER (DSO)

Laura Kravac
07375644004
laura@actionforconservation.org

DEPUTY DSO

Emma Schofield
07946064533
emma@actionforconservation.org

DESIGNATED TRUSTEE

Alex Mills
07515004270
alexcmills@gmail.com

1. ROLES AND RESPONSIBILITIES

Designated Safeguarding Officer (DSO)

- Managing all aspects of the referral process, including:
    - Referring cases of suspected abuse to the local authorities as required and supporting staff who make referrals.
    - Referring cases where a person is dismissed or has left due to risk/harm to a child to the Disclosure and Barring Services as required.
    - Referring cases where a crime may have been committed to the police as required.
    - Keeping secure records of all referrals.
- In the event of a referral, liaising with parents, teachers, case managers and designated officers at the local authority.
- Acting as a source of support, advice and expertise for all staff and volunteers with regards to matters of safety and safeguarding. The DSO should be available for team members to discuss any safeguarding concerns.
- Undergoing training to provide them with the knowledge and skills required to carry out the role. This training should be updated at least every two years.
- Encourage workplace culture where child safeguarding is a top priority, and is responsible for ensuring the organisation's safeguarding policies and procedures are known, understood, used appropriately and revised annually.

Staff and volunteers

- Having up-to-date awareness of AFC's E-Safety Policy and procedure in conjunction with AFC's Child Safeguarding Policy.
- Reporting any suspected misuse or incidents to the DSO or Deputy DSO.

- Ensuring e-safety issues are embedded in all materials given out to children and their parents/carers and discussed during workshops, events and camps.
- Ensuring children understand and follow AFC's Behaviour and Safety Guidelines for Young People.
- Communicating e-safety issues and concerns to parents through newsletters, written materials, websites and emails as appropriate.

Partner organisations or individuals

- Having access to and following AFC's E-Safety Policy in conjunction with AFC's Child Safeguarding Policy.
- Understanding how to report complaints as outlined in AFC's Child Safeguarding Policy.

2. EDUCATION AND TRAINING

Staff and volunteers

- AFC's E-Safety Policy will be made available to all staff and volunteers and discussed during induction and training, including responsibilities, procedures for reporting incidents and how to seek out information and advice.
- Formal E-safety training will be provided, where required, to staff and volunteers playing a critical role in programme planning and implementation.

Children

- All children in our programmes will be given a copy of 'AFC's Behaviour and Safety Guidelines for Young People', which includes the following:
    - Code of conduct and general expectations, including for online activities.
    - Guidelines for reporting incidents that are offensive, threatening or bullying in nature.
    - How and when to access ChildLine and the Child Exploitation and Online Protection Command (CEOP) to report abuse.
    - Additional resources for seeking support.
- Key e-safety messages will be discussed at the start of each summer camp and all Ambassador events, both in-person and remotely. A record of these discussions will be securely stored in AFC's safeguarding folder.
- Key e-safety messages will be discussed with each group during the WildED programme or during online events or presentations.

Parents and carers

- Parents/carers of children in our programmes will be made aware of the type of work we do with children and where/why we encourage internet use.
- Parents/carers of children in our programmes will be given access to our E-Safety Policy.
- Key e-safety updates and messages, including risks of internet use and practical examples of what parents/carers can do to protect their children on the internet will be sent to parents/carers via newsletters and direct emails as required. These practical examples may include:
    - Placing parental controls on home wi-fi, devices and search engines.
    - Empowering children to manage their own settings and privacy online.
    - Enforcing time settings on websites and apps to control how long and when children are online.
    - Having on-going open and honest conversations about their children's internet use.

    - Discussing the apps, social networks and websites their children use and determining which are appropriate.
- We will help parents access additional child e-safety resources such as Internet Matters, Share Aware, O2 NSPCC helpline and Thinkuknow. Links can be found in the Resource section below.

3. CYBER-BULLYING

- Cyberbullying, along with all other forms of bullying, will not be tolerated during or outside of our programmes, and it is the responsibility of all staff and volunteers to take cyberbullying incidents seriously.
- Cyber-bullying may include abusive or threatening texts, emails or messages, abusive comments made on social media, spreading rumours online, group bullying or exclusion online and encouraging a child to self-harm, among others.
- Bullying can occur across various online platforms, including social networks, apps, when playing games and through emails.
- To support children in building resilience to cyber bullying, we will show them how to block users on websites and apps, save evidence by taking screenshots of abuse and report online abuse instead of retaliating/taking action alone.
- Full details on reporting cyber-bullying incidents are set out in AFC's Child Safeguarding Policy, under 'anti-bullying.'

4. RECOGNISING ABUSE

- Please refer to AFC's Child Safeguarding Policy for a full description of the types of abuse, and recognisable physical and behavioural indicators.

5. STAFF GUIDELINES FOR APPROPRIATE INTERNET USE

Email

- AFC staff should use a secure business email account for conducting communication with children. Only staff with the appropriate level of DBS clearance are able to directly contact children and only with their permission.
- Communications between staff and a child should be conducted in a professional tone.
- AFC staff should never include a child's email address in emails with adults who are not AFC staff members and do not have the appropriate level of DBS clearance and should always 'blind copy' a child's email address when writing to groups of children.
- If a child is creating an email address specifically for AFC communications, they should be encouraged to create a non-identifiable email address.
- Emails between AFC staff and children should not be considered private and AFC reserves the right to monitor emails of staff.

Mobile Devices & Laptops

- AFC staff should not use a personal phone number to contact pupils or parents/carers without permission from the Chief Executive.
- AFC staff should not use a personal mobile device to take or store photographs or videos of children for any purpose.
- The use of AFC laptops must adhere to reasonable standards of use and staff should be aware that if they leave the charity all personal data will be wiped from the device.

Social media accounts

- Any use of social media by AFC staff should adhere to the requirements and guidelines set out in the Social Media Policy.
- Separate social media accounts should be set up and used exclusively for any communications between AFC staff and children or their family members.
- AFC staff should not refer to children by full name or give out any personal details or images which may identify them, their peers, siblings or location on social media sites or on our website. This includes a child's date of birth, address, phone number, email and school name.
- AFC staff should not accept friend requests from children on their personal social networking sites and should report any concerning interactions to the DSO.
- AFC staff should be aware of the age restriction of various social media networks and should not encourage children to join or use these networks unless they are the appropriate age.

Publishing photos of children and their work

- AFC staff should only publish photos or documentation of children that support the organisation's aims and only if we have obtained appropriate written consent from their parent/carer and verbal consent from the child.
- AFC staff should not disclose the student's full name, school or any other personal information on our website, blogs or social media platforms.

Inappropriate online activities and consequences

- All staff should be aware that illegal online activity can lead to a criminal investigation, prosecution, dismissal and barring.
- Inappropriate, but legal activity, can still lead to disciplinary action, dismissal and barring even if there is no criminal prosecution.
- If you are ever unsure if an online activity involving a child is 'appropriate' please ask the DSO.

6. VOLUNTEER GUIDELINES FOR APPROPRIATE INTERNET USE

- Volunteers will not have any direct contact with children and will otherwise adhere to the guidelines above for staff.

7. REPORTING AND RESPONDING TO INCIDENTS

- Please refer to the AFC Child Safeguarding Policy for the reporting procedure.

8. RESOURCES FOR STAFF, VOLUNTEERS AND PARENTS

- Childline: https://www.childline.org.uk/
- NSPCC: Bullying and Cyberbullying: https://www.nspcc.org.uk/preventing-abuse/child-abuse-and-neglect/bullying-and-cyberbullying/
- Safer Internet Centre: https://www.saferinternet.org.uk/professionals-online-safety-helpline
- Thinkuknow: https://www.thinkuknow.co.uk/
- Net Aware: https://www.net-aware.org.uk/

- PANTS: https://www.nspcc.org.uk/preventing-abuse/keeping-children-safe/underwear-rule/
- Shareaware: https://www.nspcc.org.uk/preventing-abuse/keeping-children-safe/share-aware/
- O2 NSPCC Helpline: https://www.o2.co.uk/help/nspcc

Policy	E-Safety Procedure
Review Dates	16/03/2018; 15/03/2019; 11/02/2020; 14/12/2020; 01/04/2022; 19/01/2023; 23/01/2024
Next review due	23/01/2025