Child E-Safety Policy

Introduction

Heal is an environmental charity that coordinates volunteer activities that involve both children and adults in the UK. Heal hosts an online community of volunteers which is deliberately diverse in age, background and other characteristics. Heal Future is Heal's youth network for people aged 30 and under.

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.

Heal 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, Heal 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.

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.

This policy applies across our organisation to all staff, trustees, volunteers, children and partner organisations and individuals we work with. Heal'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.

Purpose of this policy

The two priority objectives of this policy are:

- To demonstrate how Heal will protect children who interact with Heal's staff and volunteers online
- To provide staff, volunteers and partner organisations the overarching principles that guide our approach to safeguarding children online

Legal framework

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

- Malicious Communications Act 1988
- Children Act 1989
- United Convention of the Rights of the Child 1991

- Data Protection Act 1998
- Public Interest Disclosure Act 1998
- Communications Act 2003
- Sexual Offences Act 2003
- Children Act 2004
- Equality Act 2010
- Protection of Freedoms Act 2012
- Working Together to Safeguard Children Guidance 2018
- Data Protection Act 2018

Related policies and documents

This policy should be used in conjunction with other policies developed by Heal:

- Safeguarding Policy
- Health and Safety Policy
- Equality and Diversity Policy
- Data Protection and Privacy Policy
- Whistleblowing Policy
- Procedure for Managing Safeguarding Allegations

E-safety risks

Examples of E-safety risks include:

- 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

Actions to keep children safe online

Heal will seek to keep children safe online by:

- Ensuring that we will, with our partner organisations and schools, promote e-safety of children as the norm so that it becomes everyone's business
- Educating all Heal 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 Heal's Child Safeguarding Policy

We are committed to reviewing this policy and procedures annually.

Policy	E-Safety Policy
Next review date	3rd March 2022
Designated Safeguarding Officer	Hannah Needham, Junior Director
Signature	

Heal Child Safeguarding Procedure

Designated Safeguarding Officer (DSO)

Hannah Needham
07760993599
hannah@healrewilding.org.uk

Designated Trustee

Jan Stannard
07710171704
jan@healrewilding.org.uk

1. Designated Safeguarding Officer (DSO) role and responsibilities

The DSO is responsible for 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, the DSO is responsible for liaising with parents, teachers, case managers and designated officers at the local authority.

The DSO should act 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.

The DSO should undergo 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.

The DSO should encourage a 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.

2. Staff roles and responsibilities

All Heal staff should:

- Have up-to-date awareness of Heal's E-Safety Policy and procedure in conjunction with Heal's Child Safeguarding Policy

- Report any suspected misuse or incidents to the DSO
- Ensure that e-safety issues are considered and safety procedures embedded into materials produced by Heal for children
- Ensure that children understand and follow Heal's Child Safety Guidelines
- Communicate e-safety issues and concerns to parents through emails as appropriate
- Ensure that all partner organisations, volunteers and individuals working with Heal have access to Heal's E-Safety Policy and Child Safeguarding Policy
- Understand how to report complaints as outlined in Heal's Child Safeguarding Policy

3. Education and training

3.1 Staff

As part of their induction, all Heal staff are required to read this policy, and sign to confirm they have read it and will act in accordance with it.

All Heal staff will receive e-safety training as part of their safeguarding training and be made aware of all relevant policies and procedures and Heal's mission and commitment to safeguarding.

Staff will be trained to recognise e-safety issues and know the appropriate reporting systems for this.

Staff will receive guidance on how to respond to disclosures of abuse.

All new staff will be adequately supervised and their progress reviewed on a regular basis.

3.2 Volunteers

As part of their induction, all Heal volunteers will be provided access to a web portal containing all of Heal's policies.

Any volunteers who sign up to work on Heal Future activities must sign to confirm they have read the E-Safety Policy and will act in accordance with it.

All volunteers who sign up to work on Heal Future activities will receive e-safety training as part of their safeguarding training and be made aware of all relevant policies and procedures and Heal's mission and commitment to safeguarding.

All volunteers who sign up to work on Heal Future activities will be trained to recognise e-safety issues and know the appropriate reporting systems for this.

All volunteers who sign up to work on Heal Future activities will receive guidance on how to respond to disclosures of abuse.

All volunteers who sign up to work on Heal Future activities will be adequately supervised and their progress reviewed on a regular basis.

3.3 Children

All children that volunteer with Heal will be given a copy of Heal's Child Safety Guidelines, 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 every Heal Future event, both in-person and remotely. A record of these discussions will be securely stored in Heal's safeguarding folder.

3.4 Parents, carers and guardians

Parents, carers and guardians of children who volunteer with Heal will be made aware of the type of work we do with children and where/why we encourage internet use.

Parents, carers and guardians of children who volunteer with Heal will be given access to our E-Safety Policy

Heal 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.

4. Cyber-bullying

Cyberbullying, along with all other forms of bullying, will not be tolerated at Heal, 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
- Encouraging a child to self-harm

Bullying can occur across various online platforms, including social networks, apps, when playing games and through emails.

We will encourage children to disclose concerns about cyber-bullying to staff, their parents, carers or guardians.

Full details on reporting cyber-bullying incidents are set out in Heal's Child Safeguarding Policy, under 'anti-bullying.'

5. Recognising abuse

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

6. Staff guidelines for appropriate internet use

6.1 Email

Heal 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.

Heal staff should never include a child's email address in emails with adults who are not Heal 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 Heal communications, they should be encouraged to create a non-identifiable email address.

Emails between Heal staff and children should not be considered private and Heal reserves the right to monitor emails of staff.

6.2 Mobile devices

Heal staff should not use a personal phone number to contact children, parents, guardians or carers without permission from the DSO.

Heal staff should not use a personal mobile device to take or store photographs or videos of children for any purpose.

6.3 Social media

Separate social media accounts should be set up and used exclusively for any communications between Heal staff and children or their parents, carers or guardians.

Heal staff should not refer to children by their 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.

Heal staff should not accept friend requests from children on their personal social networking sites and should report any concerning interactions to the DSO.

Heal 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.

6.4 Publishing photos of children and their work

Heal 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, guardian or carer and verbal consent from the child.

Heal staff should not disclose the student's full name, school or any other personal information on our website, blogs or social media platforms.

6.5 Slack

Direct messages to children from Heal staff members should not be sent privately (one-to-one). Direct messages should be sent in groups that also contain the DSO and/or designated trustee. This is to ensure that the key team members responsible for safeguarding and e-safety (DSO and designated trustee) can monitor all messages sent to and by children on Slack for e-safety risks.

Heal staff members should ensure that a child's full name, email address and contact details should never be visible to any Slack users.

Heal staff members should ensure that all Slack accounts for children do not display photographs of the child. Staff should ensure that children use photographs of animals/nature, cartoons or avatars as their display photos.

Heal staff members should closely monitor group discussions in Slack to ensure that all Slack discussions contain safe, appropriate and professional language, that no inappropriate content is shared and to monitor for any e-safety risks that may harm children.

Communications between staff and a child should be conducted in a professional tone.

6.6 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.

7. Volunteer guidelines for appropriate internet use

7.1 Email

Only volunteers with the appropriate level of DBS clearance and permission from the DSO are able to directly contact children and only with their permission. The DSO and/or designated trustee must be copied into all email communications between volunteers and children.

Communications between volunteers and a child should be conducted in a professional tone.

Heal volunteers should never include a child's email address in emails with adults who are not Heal 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 adults or children.

7.2 Mobile devices

Heal volunteers should not use a personal phone number to contact children, parents, guardians or carers.

Heal volunteers should not use a personal mobile device to take or store photographs or videos of children for any purpose.

7.3 Social media

Heal volunteers should not use social media to communicate with any children that are involved with Heal, or their parents, carers or guardians.

Heal volunteers should not refer to children by their 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.

Heal volunteers should not accept friend requests from children on their personal social networking sites and should report any concerning interactions to the DSO.

Heal volunteers 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.

7.4 Publishing photos of children and their work

Heal volunteers should not publish photos or documentation of children that volunteer, visit or are associated with Heal.

Heal volunteers should not disclose the student's full name, school or any other personal information on our website, blogs or social media platforms.

7.5 Slack

Direct messages to children from Heal volunteers should not be sent privately (one-to-one). Direct messages should be sent in groups that also contain the DSO and/or designated trustee. This is to ensure that the key team members responsible for safeguarding and e-safety (DSO and designated trustee) can monitor all messages sent to and by children on Slack for e-safety risks.

If Heal volunteers see that a child's full name, email address and/or contact details are visible in Slack they must report it to the DSO immediately.

If Heal volunteers see that a Slack account for a child displays a photograph of the child, they must report it to the DSO immediately.

If a Heal volunteer sees that a Slack user is using inappropriate, unprofessional language, sharing inappropriate content or posing an e-safety risk that may harm children they must report it to the DSO immediately.

8. Reporting and responding to incidents

Please refer to the Heal Child Safeguarding Policy for the reporting procedure.

9. Resources for staff, volunteers, parents, carers and guardians

- Childline: https://www.childline.org.uk/
- NSPCC: Bullying and Cyberbulling: https://www.nspcc.org.uk/preventing-abuse/childabuse-and-neglect/bullying-and-cyberbullying/
- Safer Internet Centre: https://www.saferinternet.org.uk/professionals-online-safetyhelpline
- Thinkuknow: https://www.thinkuknow.co.uk/
- Net Aware: https://www.net-aware.org.uk/
- PANTS: https://www.nspcc.org.uk/keeping-children-safe/support-for-parents/pants-underwear-rule/
- Shareaware: https://www.nspcc.org.uk/preventing-abuse/keeping-children-safe/shareaware/
- O2 NSPCC Helpline: https://www.o2.co.uk/help/nspcc