Online safety policy

Approved by: Trustees	**Date:** September 2023
Trustee: Safeguarding and Child Protection Lead	Hugh Whitaker
Committee Governance	Board of Trustees
Sub-Committee Responsible	Children's Service Sub Committee
Lead Member of Staff: Director of Operations	Nagindra Chungh
Last reviewed on:	September 23
Next review due by:	September 24

Contents

1. Aims

Our charity aims to:

- Have robust processes in place to ensure the online safety of children, staff, volunteers and Trustees
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole charity in its use of technology
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

The 4 key categories of risk

Our approach to online safety is based on addressing the following categories of risk:

- Content – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism
- Contact – being subjected to harmful online interaction with other users, such as 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, such as 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; and
  Commerce – risks such as online gambling, inappropriate advertising, phishing and/or financial scams

2. Legislation and guidance

This policy is based on the Department for Education's (DfE) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- Searching, screening and confiscation

It also refers to the DfE's guidance on protecting children from radicalisation.
It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers/adults stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils'/children's electronic devices where they believe there is a 'good reason' to do so.

Other guidance in addition to above are available:

- Online abuse learning. 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

3. Roles and responsibilities

3.1 Board of Trustee's

The board of trustee's has overall responsibility for monitoring this policy and holding the CEO/SLT to account for its implementation.

The trustee board will make sure all staff undergo online safety training as part of child protection and safeguarding training, and ensure staff understand their expectations, roles and responsibilities around filtering and monitoring.

The trustee board will also make sure all staff receive regular online safety updates (via email, e-bulletins and staff meetings), as required and at least annually, to ensure they are continually provided with the relevant skills and knowledge to effectively safeguard children.

The trustee board will co-ordinate regular meetings with appropriate staff to discuss online safety, and monitor online safety logs as provided by the designated safeguarding lead (DSL – Operations Managers/CSL's/Director of Operations)

The trustee who oversees online safety is Hugh Whitaker

All trustees will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the Charity's ICT systems and the internet (appendix 3)
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with special educational needs and/or disabilities (SEND). This is because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable.

3.2 The Operations Managers/SLT

The operations managers /SLT is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the organisation.

3.3 The designated safeguarding lead

Charity's DSL's (Operations Mangers/CSL's/Director of Operations) are set out in our child protection and safeguarding policy as well as relevant job descriptions.

The DSL takes lead responsibility for online safety in the houses, in particular:

- Supporting the charity in ensuring that staff understand this policy and that it is being implemented consistently throughout the organisation
- Working with the operation's manager and director to review this policy annually and ensure the procedures and implementation are updated and reviewed regularly
- Taking the lead on understanding the filtering and monitoring systems and processes in place on charity devices and networks
- Working with charity and any other staff, as necessary, to address any online safety issues or incidents
- Working with the IT and Strategic Development Director to make sure the appropriate systems and processes are in place
- Ensuring that any online safety incidents are logged (see appendix 2) and dealt with appropriately in line with this policy.
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately.
- Updating and delivering staff training on online safety as needed.
- Liaising with other agencies and/or external services if necessary
- Communicating effectively on online safety in the houses to the operations managers/CSL's and/or Director of Operations.

This list is not intended to be exhaustive.

3.4 IT Support (CoopSys)

The IT support is responsible for:

- Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep children safe from potentially harmful and inappropriate content and contact online while at the houses including terrorist and extremist material.
- Ensuring that the charity's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly.
- Conduction a full security check and monitoring the Charity IT systems as required or needed.
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files.
- Ensuring that any online safety incidents are logged (see appendix 2) and dealt with appropriately in line with this policy.
- Ensuring that any incidents of cyber-bullying are dealt with appropriately.

This list is not intended to be exhaustive.

3.5 All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the Charity's IT systems and the internet (appendix 1)
- Knowing that the DSL is responsible for the filtering and monitoring systems and processes, and being aware of how to report any incidents of those systems or processes failing by reporting to CoopSys.
- Following the correct procedures by contacting CoopSys if they need to bypass the filtering and monitoring systems for educational purposes.
- Working with the DSL's to ensure that any online safety incidents are logged (see appendix 2) and dealt with appropriately in line with this policy.
- Ensuring that any incidents of cyber-bullying are dealt with appropriately
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline and maintaining an attitude of 'it could happen here'

This list is not intended to be exhaustive.

3.6 Parents

Parents are expected to:

- Notify a member of staff or the operations manager of any concerns regarding this policy or any other queries.
- Ensure their child follows the expectations of Honeypot Children's Charity.

Parents can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues? - UK Safer Internet Centre
- Hot topics - Childnet International
- Parent factsheet - Childnet International

3.7 Visitors and members of the community

Visitors and members of the community who use the Charity's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it.

4. Educating children about online safety/Remote Learning

We believe that the key to developing safe and responsible behaviours online, not only for children but everyone within our organisation. We know that the internet and other technologies are embedded in our children's lives, and we believe we have a duty

to help prepare our children to safely benefit from the opportunities the internet brings.

The Honeypot Children's Charity works with young carers and other vulnerable children and families as part of its activities.
These include:

- Residential respite care
- Social and emotional active learning residential breaks
- Community outreach sessions
- Online outreach sessions
- Online pastoral services

We aim to:

- ensure the safety and wellbeing of children and young people is paramount when adults, young people or children are using the internet, social media or mobile devices
- provide staff and volunteers with the overarching principles that guide our approach to online safety
- remind or raise relevant e-Safety messages with children routinely wherever suitable opportunities arise during their stay at Honeypot
- teach children how to use a range of age-appropriate online tools in a safe and effective way
- support children when searching the internet for information, children will be guided to use age-appropriate search engines. All use will be monitored, and children will be reminded of what to do if they come across unsuitable content.
- ensure that, as an organisation, we operate in line with our values and within the law in terms of how we use online devices.

Remote Learning

- we will endeavor to ensure that children continue to receive a good level of learning by providing a range of resources via our website.
- If our Charity chooses to communicate with children via Zoom, Teams, Skype etc then it is important that this is only carried out with the approval of the Operations Managers or Director of Operations. Children must uphold the same level of behavioural expectations, as they would in their school or when they have visited Honeypot previously.
- Any significant behavioural issues occurring on any virtual platform must be recorded, reported and appropriate sanction imposed, which may include temporarily suspending access to group online learning.
- Staff should be mindful that when dealing with any behavioural incidents, online, opportunities to discuss and repair harm will not be the same as if the child or

young person was face to face. Therefore, it may be necessary to have a discussion with the parents, regardless how minor the incident, to ensure the child is emotionally well supported.

5. Cyber-bullying

5.1 Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power.

5.2 Preventing and addressing cyber-bullying

As necessary, we will make children aware of cyber-bullying, we will ensure that children understand what it is and what to do if they become aware of it happening to them or others. We will ensure that children know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

If children bring this to the attention of the staff and something as occurred at school or home. The charity will actively discuss cyber-bullying with children, explaining the reasons why it occurs, the forms it may take and what the consequences can be. CSL's will discuss cyber-bullying with the children as needed.

Staff are also encouraged to find opportunities to use aspects of the SEAL programme to tackle cyber-bullying.

In relation to a specific incident of cyber-bullying. the DSL will consider whether the incident should be reported to the police if it involves illegal material and will work with external services if it is deemed necessary to do so.

Children's parents and school will be informed of any concerns the charity has regarding cyber-bullying that might reflect on their child/children.

5.3 Examining electronic devices

At Honeypot Charity staff discourage children to bring phones or any other electrical devices. However, if children did bring electrical devices, they will be placed in a sealed cabinet for duration of the residential break to safeguard all participants. If a child doesn't hand in their device, any authorised Charity staff member can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

- Poses a risk to staff or children, and/or
- Is identified in the Charity rules as a banned item for which a search can be carried out, and/or
- Is evidence in relation to an offence

Before a search, the authorised staff member will:

- Make an assessment of how urgent the search is, and consider the risk to other children and staff
- Explain to the child why they are being searched, how the search will happen, and give them the opportunity to ask questions about it
- Seek the child's cooperation

Authorised staff members may examine, and in exceptional circumstances erase, any data or files on an electronic device that they have confiscated where they believe there is a 'good reason' to do so.

When deciding whether there is a 'good reason' to examine data or files on an electronic device, the staff member should reasonably suspect that the device has, or could be used to:

- Cause harm, and/or
- Undermine the safe environment of the charity or disrupt breaks, and/or
- Commit an offence, and/or
- Break any of the Charity rules

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding if there is a good reason to erase data or files from a device, staff members will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material and the device will be handed to the police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

- They reasonably suspect that its continued existence is likely to cause harm to any person, and/or
- The pupil and/or the parent refuses to delete the material themselves
- If a staff member suspects a device may contain an indecent image of a child (also known as a nude or semi-nude image), they will:
- **Not** view the image
- Confiscate the device and report the incident to the DSL (or equivalent) immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on screening, searching and confiscation and the UK Council for Internet Safety (UKCIS) guidance on screening, searching and confiscation and the UK Council for Internet

Safety (UKCIS) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

Any searching of pupils will be carried out in line with:

- The DfE's latest guidance on screening, searching and confiscation
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

Any complaints about searching for or deleting inappropriate images or files on children's' electronic devices will be dealt with through the charity complaints procedure.

5.4 Artificial intelligence (AI)

Generative artificial intelligence (AI) tools are now widespread and easy to access. Staff, children and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Bard.

The Charity recognises that AI has many uses to help children learn, but may also have the potential to be used to bully others. For example, in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real.

The Charity will treat any use of AI to bully pupils in line with our safeguarding and bullying policy.

All Staff should be aware of the risks of using AI tools whilst they are still being developed and should report anyone using these inappropriately.

6. Staff using work devices outside of the charity

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- Keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol)
- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends
- Installing anti-virus and anti-spyware software
- Keeping operating systems up to date – always install the latest updates
- staff only take laptops between home and work location. No devices are left unattended or in car boots, etc.

Staff members must not use the device in any way which would violate the charity's terms of acceptable use.

Work devices must be used for work activities.

If staff have any concerns over the security of their device, they must seek advice from Operations Manager/IT support.

Honeypot Chairty Responsibility: Jeny Ray,Tel: 020 3763 150, email jenny@honeypot.org.uk

7. How the charity will respond to issues of misuse

Where a child misuses the charity's ICT systems or internet, we will follow the procedures set out in our policies. The action taken will depend on the individual circumstances, nature, and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the charity's ICT systems or the internet or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary procedures/staff code of conduct. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The charity will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

8. Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails and meetings).

By way of this training, all staff will be made aware that:

- Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse
- Children can abuse their peers online through:
    - Abusive, harassing, and misogynistic messages
    - Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
    - Sharing of abusive images and pornography, to those who don't want to receive such content
- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element

Training will also help staff:

- Develop better awareness to assist in spotting the signs and symptoms of online abuse
- Develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh up the risks

- Develop the ability to influence children to make the healthiest long-term choices and keep them safe from harm in the short term

The DSL – Operations Managers/ Children Service Leaders/Director of Operations/HR Personnel Assistant and anyone else the charity feels will undertake child protection and safeguarding training, which will include online safety. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.
Volunteers will receive appropriate training and updates, if applicable.
More information about safeguarding training is set out in our child protection and safeguarding policy.

9. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety. An incident report log can be found in appendix 2.
This policy will be reviewed annually by the Director of Operation. At every review, the policy will be shared with the board of trustees.

10. Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Staff disciplinary procedures
- General Data Protection Regulation policy
- Complaints procedure
- Anti-bullying policy and procedures
- Whistleblowing policy

Appendix 1: acceptable use agreement (staff, trustees, volunteers and visitors)

ACCEPTABLE USE OF THE CHARITY'S ICT SYSTEMS AND INTERNET:
When using the charity's ICT systems and accessing the internet at the orgnisation, or outside of the Charity on a work device (if applicable), I will not: • Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material) • Use them in any way which could harm the Charity's reputation • Access social networking sites or chat rooms • Use any improper language when communicating online, including in emails or other messaging services • Install any unauthorised software, or connect unauthorised hardware or devices to the Charity's network • Share password with others or log in to the charity's network using someone else's details • Ensure permission has been given to take photographs by Operations Director/Operations Manager/Children Services Leader. • Share confidential information about the charity, its children's or staff, or other members of the organisation • Access, modify or share data not authorised to access, modify or share • Promote private businesses, unless that business is directly related to the Charity

ACCEPTABLE USE OF THE CHARITY'S ICT SYSTEMS AND INTERNET:

I will only use the charity's ICT systems and access the internet in the organisation, or outside of the organisation on a work device, for organisation purposes such as, respite breaks, SEAL educational purposes or for the purpose of fulfilling the duties of my role.

I agree that the charity will monitor the websites I visit and my use of the charity's ICT facilities and systems.

I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside the organisation, and keep all data securely stored in accordance with this policy and the charity's data protection policy.

I will let the designated safeguarding lead (DSL) know if a child informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material.

I will always use the charity's ICT systems and internet responsibly and ensure that children in my care do so too.

Appendix 2: online safety incident report log

ONLINE SAFETY INCIDENT LOG				
Date	**Where the incident took place**	**Description of the incident**	**Action taken**	**Name and signature of staff member recording the incident**