Online Safety and Cyber Bullying Policy

Version No.	Date	Approved by	Review Frequency	Review Date
2	April 2024	Board of Trustees	+1 Year	April 2025

CONTENTS

1. AIMS

The Hebe Foundation aims to:

- Have robust processes in place to ensure the online safety of children and young people, staff, volunteers, and trustees.
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate
- Identify and support children and young people that are potentially at greater risk of harm online than others.

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 scam

2. LEGISLATION AND GUIDANCE

This policy is based on the Department for Education's (DfE) statutory safeguarding guidance, Keeping Children Safe in Education.

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.

3. ROLES AND RESPONSIBILITIES

The Board of Trustees

The board of trustees has overall responsibility for monitoring this policy and holding the Director to account for its implementation.

All Board of Trustees will:

- Ensure that they have read and understand this policy.
- Agree and adhere to the terms on acceptable use of The Hebe Foundations ICT systems and the internet.

- Ensure that, where necessary, additional oversight and monitoring of vulnerable children and young people, victims of abuse and some children and young people with SEND because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children and young people in all situations, and a more personalised or contextualised approach may often be more suitable.

The Director

The Director is responsible for ensuring:

- Staff and volunteers understand this policy, and that it is being implemented consistently throughout the foundation.
- Updating and delivering staff training on online safety.
- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems, which are reviewed and updated on a regular basis to assess effectiveness and ensure children and young people are kept safe from potentially harmful and inappropriate content and contact online while using all service, including terrorist and extremist material.
- Ensuring that the Hebe Foundations ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly.
- Conducting a full security check and monitoring the Hebe Foundations ICT systems on a regular ongoing basis.
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files.
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy.
- Ensuring that any incidents of cyber-bullying are dealt with appropriately.
- Liaising with other agencies and/or external services if necessary.

The Children's Advocate

Details of The Hebe Foundations Children's Advocate and Deputy Children's Advocate are set out in our safeguarding and child protection policy.

The Children's Advocate takes lead responsibility for online safety at The Hebe Foundation, in particular:

- Supporting the Director in ensuring that staff and volunteers understand this policy and that it is being implemented consistently throughout the foundation.
- Working with the Director and other staff, as necessary, to address any online safety issues or incidents.
- Managing all online safety issues and incidents in line with The Hebe Foundations safeguarding and child protection policy.
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy.

- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately.
- Liaising with other agencies and/or external services if necessary.

All staff and volunteers

All 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 Hebe Foundations ICT systems and the internet and ensuring that children and young people follow the Hebe Foundations terms on acceptable use.
- Working with the children's advocate to ensure that any online safety incidents are logged 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'.

Parents

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

- What are the issues? – UK Safer Internet Centre
- Hot topics – Childnet International
- Parent resource sheet – Childnet International
- Healthy relationships – Disrespect Nobody

Visitors and members of the community

Visitors and members of the community who use the Hebe Foundations ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use.

4. CYBER-BULLYING

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.

Preventing and addressing cyber-bullying

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

The Hebe Foundation will actively discuss cyber-bullying with children and young people, explaining the reasons why it occurs, the forms it may take and what the consequences can be.

All staff, volunteers and board of trustees (where appropriate) receive training on cyber-bullying, its impact and ways to support children and young people, as part of safeguarding training.

In relation to a specific incident of cyber-bullying amongst children and young people, the Hebe Foundation will take necessary actions. Where illegal, inappropriate or harmful material has been spread among children and young people, the Hebe Foundation will use all reasonable endeavours to ensure the incident is contained.

The children's advocate and/or the director will consider whether the incident should be reported to the police if it involves illegal material and provide relevant material to the police as reasonably practicable and will work with external services if it is deemed necessary to do so.

5. EXAMINING ELECTRONIC DEVICES

Staff at the Hebe Foundation have the right to examine all electronic devices issued to staff by the Foundation at request or should there be reason to believe that the device is being used for purposes other than that it was issued.

If there is a concern regarding a child or young person whilst engaging in Hebe Foundation activity, the children's advocate, deputy children's advocate and/or the director have the right to examine their electronic device in order to investigate an incident or to safeguard another child or young person.

If the children's advocate and/or director have reasonable grounds to suspect a child or young person poses a risk to staff or children and young people or there is evidence related to an offense they may:

- Make an assessment of how urgent the matter is and consider the risk to other children and young people. If the matter is not urgent, they will seek advice accordingly.
- Seek the child's or young person's cooperation in searching their device.
- Explain to the child or young person why their device is being required to be searched, giving them the opportunity to ask questions.

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 Hebe Foundation
- Commit an offence

If inappropriate material is found on the device, it is up to the children's advocate/ and/or the director 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.

If a staff member **suspects** a device **may** contain an indecent image of a child or young person (also known as a nude or semi-nude image,) they will:

- **Not** view the image

- Confiscate the device and report the incident immediately to the children's advocate and/or the director, who will decide what action to take. They will decide in line with the UK Council for Internet Safety (UKCIS) guidance.

6. ARTIFICAL INTELLIGENCE (AI)

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

The Hebe Foundation recognises that AI has many benefits 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. This includes deepfake pornography: pornographic content created using AI to include someone's likeness.

The Hebe Foundation will treat any use of AI to bully children and young people in line with our anti-bullying policy.

Staff and volunteers should be aware of the risks of using AI tools whilst they are still being developed .

7. ACCEPTABLE USE OF THE INTERNET

All staff and volunteers will be required to adhere to acceptable use of the internet while on site and/or engaging in Hebe Foundation activities.

8. STAFF USING HEBE FOUNDATION DEVICES OFF SITE

All staff and volunteers 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).
- Ensuring their hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device.
- 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 members must not use the device in any way, which would violate the Hebe Foundation's terms of acceptable use.

Work devices must be used solely for work activities.

If staff have any concerns over the security of their device, they must seek advice from the Director.

9. RESPONDING TO ISSUES OF MISUSE

Where a children or young person misuses the Hebe Foundations ICT systems or internet, we will take action depending on the individual circumstances, nature and seriousness of the specific incident, and action will be proportionate.

Where a staff member misuses the Hebe Foundations ICT systems or the internet or misuses a personal device where the action constitutes misconduct, the matter will be dealt with, and action taken accordingly. The action taken will depend on the individual circumstances, nature, and seriousness of the specific incident.

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

10. TRAINING

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

All staff members will receive refresher training at least once per year as part of safeguarding training. 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 and young people are at risk of online abuse.
- Children and young people 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 the risks up.
- Develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term.

The Children's Advocate, Deputy Children's Advocate and Director will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Board of Trustees will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

11. MONITORING ARRANGEMENTS

The Children's Advocate logs behaviour and safeguarding issues related to online safety.

The Director, at every review, will review this policy every year. The policy will be shared with the board of trustees. The review will be supported by an annual risk assessment that considers and reflects the risks pupils face online. This is important because technology, and the risks and harms related to it, evolve and change rapidly.

12. LINKS WITH OTHER POLICIES

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Staff disciplinary procedure