

Pippa's Guardians Online Safety Policy

Overview

Pippa's Guardians is committed to safeguarding and promoting the welfare of children and young people. All staff, host family members and students should understand the importance of adopting safe online practices and their role in reporting misuse, abuse, or access to inappropriate material.

An effective approach to online safety protects and educates children in their use of technology and enables us all to identify, intervene in and escalate incidents where appropriate. Promoting a safe, healthy and responsible online presence is central to this policy

This policy should be read in conjunction with Pippa's Guardians' Safeguarding Policy, Data Protection Policy and IT & Acceptable Use Policy.

This policy will be reviewed annually and updated as necessary to reflect changes in legislation, statutory guidance, technology and safeguarding practice.

Legal and Guidance Framework

This policy is informed by current UK safeguarding and online safety guidance, including:

- Keeping Children Safe in Education (KCSIE)
- Working Together to Safeguard Children
- The Children Act 1989 and Children Act 2004
- The Data Protection Act 2018 and UK General Data Protection Regulation (UK GDPR)
- The Online Safety Act 2023
- NSPCC online safety guidance
- UK Safer Internet Centre guidance

The policy will be reviewed annually by the Designated Safeguarding Lead (DSL) and Head of Compliance, or sooner if changes in legislation or guidance require it.

Designated Safeguarding Lead (DSL)

The Designated Safeguarding Lead (DSL) for Pippa's Guardians is Rose Vigers-Belgeonne.

The Deputy Designated Safeguarding Lead (DDSL) is Michelle Edwards.

Contact details:

- Rose Vigers-Belgeonne: 07731 997732 or safeguarding@pippasguardians.co.uk
- Michelle Edwards: 07802 421472 or safeguarding@pippasguardians.co.uk
- 24 hour Duty Phone: 07721 372865

The duty phone is manned by safeguarding trained Pippa's Guardians staff.

Understanding Online Safety Risks

Online safety risks can broadly be categorised into four areas:

- Content - exposure to illegal, inappropriate or harmful material, including indecent images of children, violent content, pro-self-harm or pro-eating disorder material.
- Contact - harmful online interaction with other users, including cyberbullying, grooming, coercion or exploitation.
- Conduct - personal online behaviour that increases the likelihood of, or causes, harm.
- Commerce - risks associated with online financial activity, scams, fraud and exploitation.

What Is Online Abuse?

Online abuse is any type of abuse that occurs through the internet or digital technology. Children and young people may experience cyberbullying, grooming, online sexual abuse, exploitation, emotional abuse, coercion or pressure to share nude or semi-nude images and/or videos.

Cyberbullying

Cyberbullying is bullying that takes place using digital technology, including social media, messaging apps, online gaming and mobile devices. It may include:

- Sending threatening or abusive messages
- Creating or sharing embarrassing images or videos
- Trolling or sending upsetting messages
- Excluding individuals from online groups or activities
- Creating fake accounts or stealing online identities
- Encouraging self-harm
- Pressuring a child to send sexual images or engage in sexual conversations

Grooming

Grooming involves building a relationship with a child in order to abuse or exploit them. Online grooming may occur through social media, gaming platforms, live streaming services, chatrooms or messaging apps.

Adults seeking to groom children may:

- Create false identities
- Pretend to be children or young people
- Gather information from a child's online activity
- Target children who may be vulnerable
- Encourage private communication
- Coerce or manipulate a child into sharing sexual images or meeting in person

The goal of grooming is often sexual abuse or exploitation. Any concern about grooming must be treated as a safeguarding matter and reported immediately.

Nude or Semi-Nude Images and/or Videos

The sharing of nude or semi-nude images and/or videos by children can be harmful and may constitute a safeguarding concern. Staff and host family members must not view, copy, print, share or save such imagery unless there is a clear safeguarding reason to do so. Any incident should be referred immediately to the DSL, who will assess the risk and follow current KCSIE guidance.

Emerging Online Risks

Pippa's Guardians recognises that online risks continue to evolve. Additional risks may include:

- Artificial intelligence (AI) tools and AI-generated content
- Deepfake or manipulated sexual imagery
- Encrypted messaging services and disappearing messages
- Live streaming platforms
- Online scams, fraud and financial exploitation
- Algorithm-driven harmful content
- Online radicalisation and extremist content

Possible Signs of Online Abuse

A child experiencing online abuse may demonstrate changes in behaviour, including:

- Being upset after using the internet or a mobile device
- Becoming secretive about online activities
- Spending significantly more or less time online
- Receiving numerous new messages, phone numbers or email addresses
- Appearing withdrawn, anxious or angry after online activity
- Avoiding school, friends or previously enjoyed activities
- Difficulty sleeping
- Low self-esteem

These signs do not necessarily indicate abuse, but they should prompt further consideration and, where appropriate, discussion with the DSL.

Responsibilities

Staff and Host Family Members

Staff and host family members are expected to:

- Maintain appropriate professional boundaries in online communication with students
- Promote safe and responsible online behaviour
- Participate in safeguarding and online safety training
- Record concerns accurately and promptly
- Report any online safety concern immediately to the DSL or DDSL

Students

Students should be encouraged to:

- Use the internet and digital technology safely and responsibly
- Keep personal information private - advice from Childline on Digital Footprints [here](#):
- Use privacy settings and reporting functions on apps and platforms
- Report anything online that makes them feel unsafe, uncomfortable or worried

Privacy Settings and Parental Controls

Host families are encouraged to use privacy settings, parental controls and built in internet safety features provided by internet service providers and digital platforms although we recognise that managing access to inappropriate content can be complex, as controls vary by internet provider, devices and apps, and Wi-Fi settings do not affect mobile data.

For this reason, ongoing conversations with children about online safety remain the most effective approach. The NSPCC also offers a recorded online safety workshop for parents and anyone responsible for children. [Free Online Safety Virtual Workshops | NSPCC](#)

Useful resources include:

- NSPCC Online Safety resources [here](#)
- NSPCC setting up parental/carers controls [here](#)

Procedure for Responding to an Online Safety Incident

If a member of staff or a host family member receives a report of suspected online abuse, they must:

- Listen carefully and reassure the child that they have done the right thing by reporting the concern.
- Record the disclosure as soon as possible, using the safeguarding concern form that can be found [here](#)
- Report the concern verbally to the DSL or DDSL as soon as is practically possible.

- Preserve relevant evidence where appropriate, such as screenshots, but do not unnecessarily view, copy or share illegal or harmful material.

The DSL will assess the concern and determine the appropriate course of action, which may include:

- Liaising with the student's school DSL
- Contacting parents or carers where it is safe and appropriate to do so
- Referring the matter to children's services
- Reporting the matter to the police via 101, or 999 in an emergency
- Providing ongoing support to the student

Police Involvement

Police involvement may be appropriate where:

- The incident involves an adult
- There is evidence or suspicion of grooming, coercion, blackmail or exploitation
- A child may be at immediate risk of harm
- The content depicts sexual acts involving a child under 13
- The material is violent, exploitative or otherwise indicates a serious safeguarding concern
- The child is presenting as suicidal, self-harming or otherwise at significant risk

Immediate risk of harm should be reported to the police by dialling 999.

Support for Children and Staff

Pippa's Guardians will work with schools, families, host families and relevant professionals to ensure that children affected by online abuse receive appropriate support. This may include emotional support, education about online risks and assistance with reporting harmful content.

Staff or host family members who have been exposed to distressing online content in the course of their safeguarding duties will also be offered appropriate support.

Data Protection and Record Keeping

Information relating to online safety incidents will be processed in accordance with the Data Protection Act 2018 and UK GDPR.

- Safeguarding records will be stored securely and accessed only by authorised personnel.
- Information will be shared on a need-to-know basis where necessary to safeguard a child or comply with legal obligations.
- Records will be retained in line with the organisation's data retention schedule.
- Confidentiality cannot be guaranteed where information needs to be shared to protect a child from harm.

Policy Information	
Policy Version:	V11
Date of Policy:	10 th July 2026
Date of Policy Review:	10 th July 2027
Review responsibility:	Imogen Trevethan
Policy approved by:	Pippa's Guardians Senior Leadership Team