



Digital Safeguarding Policy

Last review: 12.6.26

Reviewed by: Amy Holgate, DSL

Approved by: Board Safeguarding Lead, Katherine Conlon

Next review: 12.6.27

Digital safeguarding concerns should follow the operational steps in the Children's Safeguarding Procedure (recognise, respond, record, report). Once escalated, the DSL determines whether the concern meets child safeguarding thresholds, adult safeguarding thresholds, or both, and applies the relevant policy.

This policy should be read alongside NeonDaisy's:

- Children's Safeguarding Policy and Procedure
- Adult Safeguarding Policy and Procedure
- NeonDaisy 'Practice Handbook: What's Under the Surface'
- Behaviour Code
- Data Protection, Privacy and Device Use Policies

It applies to all adults interacting with NeonDaisy online, including parents/carers in the Facebook community or WhatsApp groups, adults contacting us via email or social media, facilitators, freelancers, volunteers, moderators, partner-venue staff and any adult communicating digitally with NeonDaisy, as well as any digital contact initiated by children or young people (whether accidental, brief, or via public channels).

Digital safeguarding statement

NeonDaisy is committed to maintaining safe, respectful and neuro-affirming digital spaces. Digital safeguarding applies across all online platforms we use, including email, social media, parent/carer messaging groups and digital creative submissions (submitted only via parents/carers). We recognise that neurodivergent young people and adults may face increased digital risks, including misinterpretation, coercion, platform-hopping and algorithmic harm.

NeonDaisy does not provide crisis support through any digital channel, and public-facing platforms are not safeguarding reporting routes.

We do not communicate directly with young people online; all communication occurs in person or via their parent or carer.

Adults use only approved communication channels, do not private-message participants, and do not save or forward digital content unless directed by the DSL.

Digital safeguarding is everyone's responsibility.

1. Purpose of this policy

This policy sets out how NeonDaisy ensures:

- Safe digital communication
- Safe online communities
- Safe use of messaging apps
- Safe use of social media
- Safe handling of digital safeguarding concerns
- Clear boundaries for adults
- Clear expectations for moderators and staff
- Clear escalation routes
- Proportionate information sharing
- Safe record keeping

Digital safeguarding applies across all NeonDaisy digital spaces.

2. Principles

NeonDaisy's digital safeguarding practice reflects the organisational safeguarding principles set out in the Children's and Adults' Safeguarding Policies, including child centred practice, neuro affirming practice, trauma informed practice, contextual safeguarding, anti adultification, cultural safety and proportionate systems.

NeonDaisy commits to:

- Creating safe, respectful, neuro affirming digital spaces
- Maintaining clear, concrete communication
- Ensuring adults understand digital boundaries
- Ensuring moderators follow safe practice
- Ensuring staff do not investigate safeguarding concerns
- Ensuring public facing channels are not used for crisis support
- Ensuring proportionate information sharing
- Ensuring safeguarding overrides confidentiality
- Ensuring digital communication is professional and boundaried
- Ensuring adults maintain safe expectations when discussing young people online
- Ensuring digital safeguarding concerns are escalated immediately

3. Legal and regulatory framework

NeonDaisy's digital safeguarding practice is aligned with:

- Online Safety Act 2023
- Children Act 1989 and 2004
- Working Together to Safeguard Children 2026
- Care Act 2014
- Mental Capacity Act 2005
- Data Protection Act 2018 and UK GDPR
- ICO Children's Code
- Equality Act 2010
- Local safeguarding partnership guidance
- NSPCC online safety guidance
- Barnardo's Online Risk Guide (4Cs model)

NeonDaisy is a small CIC. Safeguarding systems are proportionate to scale while meeting statutory expectations.

3.1 Online Safety Act 2023

NeonDaisy meets its responsibilities by:

- Moderating or supervising all digital spaces used by NeonDaisy
- Monitoring user-generated content for harmful or illegal content
- Removing harmful content where possible and escalating concerns to the DSL
- Ensuring no young person is required to create an account below the digital age of consent
- Ensuring staff and moderators do not investigate concerns
- Ensuring all digital communication routes are risk-assessed and proportionate
- Signposting to emergency services where immediate risk is identified

NeonDaisy does not provide crisis support through any digital channel. We provide permanent signposting to crisis support services where appropriate for out of hours.

The DSL is available for digital escalation during delivery hours. When unavailable, the Deputy DSL provides cover.

3.2 Digital age of consent and platform age rules

NeonDaisy follows UK digital age-of-consent requirements:

- The UK digital age of consent is 13

- Young people under 13 must not create accounts on platforms requiring personal data
- WhatsApp's minimum age in the UK is 13
- Young people under 13 must not be added to WhatsApp groups
- NeonDaisy does not use platforms requiring users to be 16+ or 18+

NeonDaisy does not communicate directly with young people on any platform.

4. Digital wellbeing

NeonDaisy supports digital wellbeing by:

- Encouraging balanced use of digital tools
- Supporting young people, through in-person work and via parents and carers, to recognise when digital spaces feel unsafe or overwhelming
- Encouraging breaks from digital spaces where this supports regulation and safety
- Supporting parents and carers to understand digital risks and how they may affect neurodivergent young people
- Ensuring staff model healthy digital boundaries

NeonDaisy also holds open, facilitated discussions with young people in groups about digital safety, online behaviour, boundaries, manipulation, platform risks and how digital environments interact with neurodivergence, race and gender.

4.1 Digital literacy

NeonDaisy supports digital literacy by:

- Helping young people, in sessions and projects, to understand online risks in concrete, neuro-affirming ways
- Supporting parents and carers to understand digital safety and platform features
- Encouraging critical thinking about online content
- Supporting young people and adults to recognise misinformation, disinformation and AI created content
- Encouraging safe sharing practices
- Supporting young people and adults to understand privacy settings and data use

4.2 Online harms (Barnardo's 4Cs model)

NeonDaisy recognises the four categories of online harm:

Content risk - exposure to harmful or age-inappropriate material.

Contact risk - unsafe interaction with others online, including grooming, coercion or pressure.

Conduct risk - harm arising from a young person's own online behaviour, including sharing personal information or images.

Contract/Commercial risk - risks from commercial exploitation, including scams, data harvesting and targeted advertising.

Any online harm is escalated to the DSL.

5. Grooming and exploitation indicators

NeonDaisy recognises that grooming and exploitation online may involve:

- Flattery or excessive praise
- Secrecy or requests to keep communication private
- Pressure to move to encrypted platforms
- Pressure to delete messages
- Gifts, money or incentives
- Attempts to isolate the young person
- Attempts to undermine parents or trusted adults

Any grooming indicators are escalated immediately to the DSL.

5.1. Platform-hopping risk

NeonDaisy recognises that unsafe adults may attempt to:

- Initiate contact on one platform
- Move the young person to another
- Then move to encrypted or private channels

NeonDaisy mitigates this by:

- Prohibiting private one-to-one messaging between staff and participants
- Prohibiting unsupervised platform changes in any NeonDaisy-linked space
- Ensuring moderators escalate concerns immediately
- Supporting young people, in person, to recognise unsafe requests to move platforms
- Supporting parents and carers to recognise and respond to unsafe digital requests

NeonDaisy does not communicate directly with young people online.

6. Algorithmic and systemic risk

NeonDaisy recognises that online platforms may expose young people to harmful or distressing content through algorithms and targeted features. This may include amplification of extreme material or reinforcement of racialised, gendered or neurodivergent stereotypes.

NeonDaisy mitigates this by supporting young people, in person and via parents/carers, to understand how algorithms shape content, reviewing harmful disclosures immediately and escalating concerns to the DSL.

7. Digital resilience

NeonDaisy supports young people to recognise unsafe digital behaviour, understand their rights online and seek help from trusted adults. We encourage blocking, reporting and safe exiting from harmful situations, and support young people to identify manipulation, pressure or boundary-crossing online.

NeonDaisy reinforces these messages through in-person work and supports parents and carers to continue them at home.

8. Specific vulnerabilities

NeonDaisy recognises that some young people may experience additional digital vulnerabilities because of how online environments interact with neurodivergence, gender and lived experience. These may include misinterpretation, pressure to respond, or being targeted through communication differences.

NeonDaisy responds by maintaining clear, concrete communication, predictable boundaries and neuro-affirming interpretation, and by supporting young people and parents/carers to recognise unsafe digital behaviour and trust their discomfort.

9. Neurodivergent facilitators as digital role models

NeonDaisy's facilitators are neurodivergent adults who model safe, bounded and respectful communication about digital safety. They do not communicate digitally with young people. Their digital communication is only with parents and carers, partner organisations and other adults.

9.1 Facilitators as digital role models

Facilitators model:

- Clear, concrete communication when discussing digital safety with parents and carers
- Predictable boundaries in digital-related work
- Neuro-affirming interpretation of behaviour and communication
- Professional tone and respectful digital conduct
- Avoidance of over-identification or oversharing
- Avoidance of therapeutic advice or crisis support

9.2 Safe digital practice for staff and facilitators

All staff and facilitators follow safe digital practice to protect young people, at-risk adults and the organisation. Digital communication is professional, bounded and conducted only through approved organisational channels.

Staff and facilitators must:

- Use approved organisational channels for all digital communication
- Avoid private one-to-one messaging with parents or carers on personal accounts
- Keep any necessary project-related communication within organisational systems
- Avoid using personal devices or personal cloud services for communication, storage or forwarding
- Create or retain digital evidence only when directed by the DSL
- Store digital information securely in line with UK GDPR and the retention schedule
- Maintain secure access (strong passwords, multi-factor authentication, no shared logins)
- Report any suspected data breach to the DSL immediately
- Avoid discussing young people digitally except where essential for safeguarding and in line with the Children's and Adults' Safeguarding Procedures and the Data Protection and Privacy Policy
- Escalate digital safeguarding concerns immediately and record them in the same way as in-person concerns

10. Staff social media use

Staff (including freelancers or volunteers working for NeonDaisy) must:

- Not "friend", follow or connect with parents, carers or young people on personal accounts
- Not comment on posts about NeonDaisy work from personal accounts

- Not share images, screenshots or content from NeonDaisy spaces on personal profiles
- Not screenshot or save content from NeonDaisy digital spaces to personal devices
- Not discuss NeonDaisy work, families or young people on personal social media

12. Private Facebook community (parents and carers)

12.1 Admission rules

Members must:

- Live in Bristol, Bath, South Gloucestershire, North Somerset or surrounding areas
- Be a parent or carer of a neurodivergent girl or gender-nonconforming young person
- Agree to the group rules
- Answer admission questions honestly

12.2 Group rules / description

Members must:

- Treat others with respect
- Avoid posting identifiable information about children
- Avoid sharing screenshots outside the group
- Avoid promoting their own business unless free or low-cost and relevant
- Avoid giving professional advice
- Avoid sharing harmful or unsafe content
- Avoid posting age-inappropriate content or content rated above 12A
- Use #admin to alert moderators
- Avoid mentioning professionals by name

Members may:

- Share experiences
- Share recommendations without vested interest
- Arrange informal meetups at their own risk
- Connect privately at their own risk

NeonDaisy states clearly in the group description that:

- NeonDaisy is not responsible for any private connections, conversations or meetups arranged between members outside the group and they connect outside the group at their own risk.

- NeonDaisy does not endorse or verify services shared by members.
- NeonDaisy clearly states in the group description and rules that we are not a crisis service and do not monitor messages outside working hours.

12.3 Moderator responsibilities

Moderators must:

- Apply group rules
- Remove unsafe content
- Escalate safeguarding concerns immediately
- Pause comments if a discussion becomes unsafe
- Avoid providing advice
- Avoid investigating
- Avoid private messaging members
- Avoid saving or forwarding content unless directed by the DSL

Moderators are not DBS-checked adults and do not make safeguarding decisions. They do, however, have safeguarding responsibilities: recognising digital concerns, pausing unsafe discussions and escalating immediately to the DSL.

Moderators receive a role-specific induction covering digital safeguarding, recognising concerns, escalation routes and boundaries. Moderators follow a weekly rota to ensure predictable oversight of the group.

A shared moderator communication channel is used to raise posts of concern, request cover and discuss issues proportionately. The DSL is part of this channel and provides regular guidance and reviews emerging themes.

12.4 Safeguarding concerns in the parent Facebook community

Moderators may encounter posts indicating risk to a child or adult. These include parents/carers sharing information about:

- A child experiencing suicidal thoughts or self-harm
- A child being groomed, exploited or contacted unsafely online
- A child causing danger to a parent or sibling
- A parent describing an abusive or unsafe partner
- A parent experiencing neurodivergent dysregulation, shutdown or burnout that affects their safety
- A parent experiencing chronic illness, carer stress or being a lone parent without support
- Any situation where a child or adult may be at risk of significant harm

When a concern is posted, moderators must:

- Avoid providing emotional support, reassurance, advice or asking follow up questions
- Avoid private messaging
- Provide signposting to relevant urgent services/support only and NeonDaisy mental health website signposting page
- Pause comments
- Escalate immediately to the DSL
- **Digital concerns follow the Children's Safeguarding Procedure**

12.5 Moderators' access to parent information

Moderators may see names behind anonymous posts and personal disclosures shared by parents/guardians in the private Facebook group. Moderators do not reveal, reference or act on information gained through moderation in any other NeonDaisy context. It is not used to inform facilitation, relational practice or support for children unless a safeguarding concern is present.

13. Digital contact routes

13.1 Staff response to any digital safeguarding concern (public, DM or email)

If a safeguarding concern is received through any digital route, staff must:

- Acknowledge the message briefly using clear, concrete language
- Avoid providing advice, reassurance or therapeutic support
- Avoid extended conversation
- Avoid private messaging on personal accounts
- Record observable facts only
- Escalate immediately to the DSL
- Signpost to emergency services if there is immediate risk

Staff do not investigate concerns and do not use digital channels for ongoing communication with young people or at-risk adults.

13.2 Public channels (Instagram, Facebook page, LinkedIn)

Public channels are used only for information, updates and community engagement. Staff do not provide support or advice through public comments.

If a safeguarding concern is posted publicly, staff follow the steps in 13.1.

NeonDaisy states clearly on all public channels that we are not a crisis service and cannot monitor messages outside working hours.

13.3 Direct messages (DMs) to organisational accounts

Direct messages sent to NeonDaisy's organisational accounts (e.g., Instagram DM, Facebook DM, LinkedIn messages) are not public, but they remain non-support channels.

If a safeguarding concern is received via DM, staff follow the steps in 13.1.

Staff do not use DMs for ongoing communication with young people.

13.4 Email (general organisational inbox)

The organisational inbox is monitored only during delivery hours and is not a crisis service. Access is limited to staff who have completed safeguarding training.

14. WhatsApp groups for parents and carers

WhatsApp groups are used only for session information, logistics and introductions. Groups are created with prior consent and are deleted after the event or project.

NeonDaisy ensures:

- Chat safety settings are set to maximum, including disabling media auto-download
- Group rules and boundaries are shared in advance
- No young people are added to WhatsApp groups
- Only organisational accounts are used
- Only staff are group admins
- Parents and carers cannot add or remove members

Parents and carers must avoid identifiable information, screenshots and professional advice.

Facilitators must use professional tone, avoid private messaging and escalate concerns to the DSL.

WhatsApp is not a safeguarding reporting route.

15. WhatsApp groups for NeonDaisy teams

Team WhatsApp groups are used for:

- Session planning
- Logistics
- Sharing links
- Coordination

NeonDaisy ensures:

- Chat safety settings are set to maximum, including disabling media auto-download
- Only staff are group admins
- Team members do not add or remove members unless authorised
- Groups are not used to discuss young people unless essential for immediate safeguarding, and then use first initials only
- If used for immediate safeguarding, the concern is transferred to the formal safeguarding log as soon as possible
- Partner-organisation staff may be added where needed for joint delivery
- Screenshots are not shared outside the group
- No photos of young people shared on the group
- Sensitive information is not shared unless proportionate and in line with safeguarding procedures

Team members must use professional tone and escalate concerns to the DSL.

16. Young people contributors (newsletter, magazine, creative submissions)

Young people may contribute artwork, writing, stories, lived experience, photos or videos. They are asked to do this through their parents or carers, who must submit it themselves via a Jotform form or email from their own email address.

NeonDaisy ensures:

- Young people know contributions are voluntary
- Young people can withdraw consent unless legally restricted
- Content is reviewed by a DBS-checked adult before publication
- Safeguarding concerns in submissions are escalated immediately
- Identifying details are removed unless explicit consent is given
- Parents/carers give consent for use of first name and age
- Content is stored securely and deleted after the retention period
- No young person is contacted privately about submissions

17. Personal devices in groups

Adults do not use their personal devices for photos, filming or communication with young people in any NeonDaisy space (in person or online). Photos and film are taken only on NeonDaisy devices as pre-arranged, with advance consent from both parents/carers and young people. We avoid asking for consent in the moment, as young people may feel pressured to agree on the spot.

The comfort and safety of young people always take priority over promotion or content creation. Images are stored securely in line with NeonDaisy's Data Protection procedures.

Young people may have their own phones in the space. A shared agreement, developed with the group, sets expectations for phone use, including sensory needs, mixed-age considerations, self-care and respectful boundaries. A simple flowchart helps young people decide when and how to use their phones safely and appropriately.

18. Youth-produced sexual imagery

NeonDaisy recognises that digital spaces may expose young people to sexualised content or requests.

If any adult becomes aware of:

- Sexualised images of a young person
- Descriptions of sexualised images
- Requests for images
- Threats to share images
- Demands for money or coercion (sextortion)
- References to OnlyFans, pornography or sexual exploitation involving a young person

Staff must:

- Not download, save, crop, forward or screenshot the content
- Not ask the young person to resend, describe or explain the image
- Escalate immediately to the DSL

Any sexualised image of a person under 18 is treated as child sexual abuse material.

Follow the Children's Safeguarding Procedure.

19. Digital safeguarding concerns

Digital safeguarding concerns include any online communication, content or behaviour that may indicate risk to a young person, an at-risk adult or the wider community. These concerns may arise across public channels, direct messages, email or organisational platforms as listed above:

- Disclosures via messaging
- Concerning posts in the Facebook group
- Concerning emails

- Concerning WhatsApp messages
- Concerning direct messages
- Contact from a young person via public or private digital channels
- Contact from an at-risk adult via public or private digital channels
- Concerning content shared by parents on behalf of young people
- Concerning behaviour by adults online
- Patterns of unsafe digital behaviour across platforms

Follow the Children’s Safeguarding Procedure

20. Responding to digital incidents

When a digital safeguarding concern arises, staff and moderators must:

- Not delete content unless necessary to prevent further harm
- Not screenshot content unless directed by the DSL
- Not download, save, crop or forward content
- Not investigate or contact the person involved
- Not attempt to resolve the issue themselves

Follow the Children’s Safeguarding Procedure and log for all next steps, i.e., record observable information only (platform, username, date/time, what was seen) and escalate immediately to the DSL

21. Low-level digital concerns

Low-level digital concerns apply to any adult interacting with NeonDaisy online, including staff, freelancers, volunteers, moderators, parents/carers and partner organisation staff.

Low-level digital concerns relate to adult behaviour in digital spaces that feels “off”, blurs boundaries or suggests emerging risk, but does not meet the threshold for a safeguarding referral. These concerns help identify early signs of poor judgement, boundary-crossing or emerging risk online.

Examples include:

- Over-familiar or inappropriate tone
- Repeated minor breaches of group rules
- Adults seeking personal or informal contact with staff
- Boundary-testing behaviour
- Comments that misinterpret or adultify young people

- Patterns of attention-seeking, triangulation or attempts to draw staff into extended digital exchanges

Low-level concerns are:

- Reviewed by the DSL
- Monitored for patterns across platforms
- Used to prevent escalation

Digital low-level concerns do not require investigation.

Follow the Children's Safeguarding Procedure

22. Record keeping

NeonDaisy keeps only the minimum digital information required for delivery, learning and safeguarding.

NeonDaisy:

- Keeps general communications for three months after the project
- Does not save content to personal devices
- Deletes digital content after the retention period
- Records general engagement themes where useful for learning
- Stores safeguarding records separately in line with the Children's and Adults' Safeguarding Procedures and the Data Protection and Privacy Policy

23. Information sharing

NeonDaisy shares information:

- Proportionately
- On a need-to-know basis
- Using secure systems
- In line with UK GDPR

Safeguarding overrides confidentiality. Information is shared only when necessary to protect a child or adult from harm, and decisions are made by the DSL or Deputy DSL.

NeonDaisy ensures that:

- Only staff with a legitimate role in managing the concern receive information
- Information shared is limited to what is essential for safety
- Neuro-affirming interpretation is applied to avoid misreading behaviour or communication

- Racialised, gendered or contextual factors are considered when assessing risk
- Records include the rationale for sharing or not sharing information

Adults and young people are informed when information must be shared unless doing so increases risk. Where informing them may escalate danger, increase distress or compromise safety planning, the DSL records the justification for withholding notification.

Information is shared with partner organisations only when proportionate, necessary and in line with safeguarding procedures.

24. Device use, storage and data protection

Digital safeguarding practice follows NeonDaisy's Data Protection and Privacy Policy.

NeonDaisy ensures that:

- Staff use organisational devices or accounts for NeonDaisy work
- Content from NeonDaisy digital spaces is not stored on personal devices
- Devices used for NeonDaisy work have appropriate security settings enabled
- Information is stored on secure, password-protected systems
- Access to digital content is limited to staff who require it for their role
- Content is deleted after the retention period
- Sensitive information is shared only when proportionate and in line with safeguarding procedures

25. Governance and oversight

NeonDaisy ensures proportionate governance and oversight of digital safeguarding across all delivery.

NeonDaisy:

- Ensures regular DSL oversight of digital spaces aligned with delivery hours
- Reviews digital safeguarding logs and emerging patterns across platforms
- Provides annual safeguarding reporting to the Board Safeguarding Lead
- Reviews this policy annually
- Shares learning from incidents proportionately
- Ensures alignment with partner organisations where relevant
- Ensures moderators receive appropriate guidance and oversight
- Escalates significant concerns to the Board Safeguarding Lead where required
- Ensures digital safeguarding is included in staff induction and annual safeguarding refreshers

- Ensures the DSL maintains specialist training in digital harms, online evidence handling and emerging risks
- Ensures digital concerns follow the Children's Safeguarding Procedure

26. Transparency, data minimisation and parental rights

NeonDaisy is transparent about what digital information is collected, why it is collected, who can access it, how long it is kept and how parents, carers or young people can request deletion or correction.

NeonDaisy collects only the minimum digital information necessary to deliver programmes safely and proportionately. Digital information is stored securely, accessed only by staff who require it for their role, and retained in line with NeonDaisy's Data Protection and Privacy Policy.

Parents, carers and young people have the right to:

- Request access to digital information held about them
- Request correction of inaccurate information
- Request deletion where appropriate
- Understand how digital information is used in safeguarding contexts

Safeguarding overrides confidentiality. Where information must be shared to protect a child or adult, NeonDaisy explains this clearly unless doing so increases risk.

NeonDaisy does not use automated decision-making or profiling tools that affect young people. No automated system is used to assess risk, allocate support or make safeguarding decisions.

Digital safeguarding concerns follow the Children's Safeguarding Procedure