Meadow Pathways Wellbeing and Education Cornwall (MPWEC)

Online Safety Policy

Education other than at School (EOTAS)

Responsibility to update: Zoe Waitz and Michelle Pascoe
Applies to: All staff, contractors, volunteers and visiting professionals working with children and young people (CYP) engaged in Meadow Pathways EOTAS packages (including tuition in homes, community venues and online).

Version No: 1
Date: September 2026
Review Date: September 2027

About This Policy

This is a new policy, introduced in September 2026 as Meadow Pathways begins to offer online sessions alongside our home, community and outdoor provision. It reflects Keeping Children Safe in Education (KCSIE) 2026, Working Together to Safeguard Children 2026, and the DfE's voluntary national standards for non-school alternative provision.

Introduction

Technology is part of every young person's life. It brings opportunities for learning and connection, and it also brings risks. Meadow Pathways Wellbeing and Education Cornwall is committed to keeping children and young people safe online, both during our sessions and by helping them develop the knowledge and confidence to stay safe in their wider lives.

This policy sets out how we:

- deliver online sessions safely;
- manage the use of technology during all our sessions;
- teach young people about online safety; and
- respond when something goes wrong.

It should be read alongside our Safeguarding and Child Protection Policy, Safer Working Practice Guidance, Staff Conduct Policy, Anti-Bullying Policy and Data Protection Policy.

Legal and Statutory Framework

- Keeping Children Safe in Education (KCSIE) 2026
- Working Together to Safeguard Children 2026
- Online Safety Act 2023
- UK GDPR and the Data Protection Act 2018
- Counter-Terrorism and Security Act 2015 (Prevent duty)
- Equality Act 2010
- UK Council for Internet Safety (UKCIS) guidance: Sharing nudes and semi-nudes – advice for education settings working with children and young people
- DfE Voluntary National Standards for Non-School Alternative Provision (2025)

The Four Areas of Online Risk

In line with KCSIE 2026, we recognise four areas of online risk:

- **Content:** being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, misinformation and disinformation, racism, misogyny, self-harm and suicide content, radicalisation and extremism.
- **Contact:** being subjected to harmful online interaction with other users, such as peer pressure, grooming, or adults posing as children or young adults to groom or exploit them.
- **Conduct:** personal online behaviour that increases the likelihood of, or causes, harm – such as making, sending and receiving explicit images (including nudes and semi-nudes and AI-generated or "deepfake" images), and online bullying.
- **Commerce:** risks such as online gambling, inappropriate advertising, phishing and financial scams.

Young people with SEND, and those who have experienced trauma, may be more vulnerable to these risks and may find it harder to recognise or report them.

Roles and Responsibilities

- **Directors (Michelle Pascoe and Zoe Waitz):** make sure this policy is in place, resourced and reviewed, and that online sessions are delivered safely.
- **Designated Safeguarding Lead (Michelle Pascoe):** leads on online safety, including responding to online safety concerns, overseeing arrangements for online sessions, and keeping up to date with emerging risks such as artificial intelligence.
- **All staff:** follow this policy, model safe and professional use of technology, supervise technology use during sessions, and report concerns to the DSL straight away.
- **Parents and carers:** support safe online sessions at home (see below), and talk to us about any online safety concerns.
- **Young people:** are supported to use technology safely and respectfully, and to tell a trusted adult if something online worries them.

Online Sessions

Online sessions are only offered where they have been agreed with the young person, their parent or carer, and the commissioning school or local authority, and where they are in the young person's best interests – for example as part of a blended package, or where a young person is not yet able to attend in person.

Before sessions start

- An online session agreement is shared with the parent or carer, setting out how sessions work and what is expected (see Appendix A).
- Staff have up-to-date contact details for the parent or carer, the young person's home address, and emergency contacts, so that help can be sent if needed.
- Session times are agreed in advance and recorded on the timetable.

The platform

- Sessions take place only on Meadow Pathways' approved platform (Microsoft Teams, through Meadow Pathways' Microsoft 365 account), using an organisation account.
- Staff never use personal accounts, personal phone numbers, social media or other apps to contact young people.
- Meeting links are sent to the parent or carer's email address, not directly to the young person, unless otherwise agreed.
- Meetings are set up so that the member of staff is the organiser and controls who can join. Young people cannot start meetings or private chats with staff outside agreed session times.

During sessions

- A parent or carer must be at home, or otherwise responsible for the young person, for the duration of any live online session.
- Staff work from a quiet, neutral, professional space with a plain or blurred background, dress appropriately, and make sure no one else can see or hear the session.

- Young people should join from a shared or open space in the home rather than a bedroom, wherever possible. If this is not possible, the camera should face a neutral wall, and this is agreed with the parent or carer.
- Cameras are optional for young people. We take a trauma-informed approach and never pressure a young person to turn their camera or microphone on.
- The same professional boundaries apply online as in person, as set out in the Staff Conduct Policy and Safer Working Practice Guidance.
- Attendance is recorded for every online session, and any unexplained absence is followed up in the same way as an in-person session.

Recording

Online sessions are not recorded unless there is a clear reason, this has been agreed in writing in advance with the parent or carer (and the young person where appropriate), and the recording is stored on Meadow Pathways' secure SharePoint and deleted when no longer needed. Staff and young people must never record sessions on personal devices.

If a concern arises during an online session

- Concerns raised during an online session are dealt with in the same way as any other safeguarding concern: report to the DSL immediately, in line with the Safeguarding and Child Protection Policy.
- If a young person is in immediate danger, staff call 999, giving the young person's address, and then contact the parent or carer and the DSL.
- Staff should not end the call abruptly if a young person is distressed or making a disclosure, unless continuing would put them at greater risk.
- If anything inappropriate is seen or heard in the young person's home, the session is ended calmly and the DSL informed.

Technology Use in Face-to-Face Sessions

- Meadow Pathways does not provide internet access for young people at community venues, and we do not allow young people to use staff members' personal devices.
- Where a young person uses a Meadow Pathways device, it has appropriate filtering in place and its use is supervised.
- Where a young person uses their own phone or device during a session, its use is agreed as part of their plan, and staff supervise it in the same way as any other activity.
- Staff follow the Safer Working Practice Guidance on the use of personal devices, photographs and images.

Nudes and Semi-Nudes

The making or sharing of nude or semi-nude images by anyone under 18 is treated as a safeguarding matter, whatever the technology used – including AI-generated, digitally altered or "deepfake" images. In line with UKCIS guidance, staff must:

- never view, copy, print, share, save or forward the image, and never ask a young person to show or send it;
- reassure the young person, and not make them feel ashamed or in trouble;

- report to the DSL immediately, who will decide on next steps, including whether to involve MASSH or the police.

Young people can be supported to use Childline and the Internet Watch Foundation's **Report Remove** tool to get nude images of themselves removed from the internet.

Online Bullying, Grooming, Exploitation and Radicalisation

- Online bullying is responded to under our Anti-Bullying Policy.
- Any concern that a young person is being groomed, exploited or radicalised online is reported to the DSL immediately, in line with the Safeguarding and Child Protection Policy and our Prevent duty.
- Concerns about online sexual abuse can also be reported to the National Crime Agency's CEOP Safety Centre.

Artificial Intelligence

Staff are alert to artificial intelligence (AI) as an emerging safeguarding risk, including AI-generated images and videos, chatbots and misinformation. Any AI-generated content involving a child that is sexual, abusive or harmful is treated as a safeguarding concern and reported to the DSL. Staff do not enter any personal information about young people into AI tools.

Teaching Online Safety

Online safety is taught as part of our PSHE and RSHE curriculum, adapted to each young person's age, needs and understanding. It covers how to stay safe, how to recognise risks, healthy online relationships, the law around sharing images, misinformation, and where to get help. We support parents and carers with guidance on privacy settings, parental controls and talking to their children about online safety.

Staff Use of Technology and Social Media

- Staff must not connect with, follow or message young people or their families on personal social media.
- Staff must not post anything about young people, families or their work with Meadow Pathways on personal social media.
- All work communication takes place through Meadow Pathways' organisation email and approved systems.
- Staff must protect their devices and accounts with strong passwords and two-factor authentication, and report any lost device or suspected security breach to the Directors immediately.

Data Protection

Information about young people is handled in line with our Data Protection Policy and Privacy Notice. Online sessions and any related records are stored only on Meadow Pathways' secure systems.

Training

All staff receive online safety training at induction and as part of their annual safeguarding update, including how to deliver online sessions safely, the four areas of risk, and how to respond to incidents.

Useful Contacts

- **Meadow Pathways DSL:** Michelle Pascoe – 07563 862530 – Michelle.Pascoe@meadowpathwayscornwall.com
- **Deputy DSL:** Zoe Waitz – 07563 855070 – Zoe.Waitz@meadowpathwayscornwall.com
- **Emergency:** 999
- **Cornwall MASSH:** 0300 123 1116 (out of hours 01208 251300)
- **CEOP Safety Centre:** www.ceop.police.uk/safety-centre
- **Childline (including Report Remove):** 0800 1111 – www.childline.org.uk
- **Report Harmful Content:** reportharmfulcontent.com

Monitoring and Review

This policy is reviewed annually by the Directors, or sooner if guidance changes, new technology or risks emerge, or following an incident.

Appendix A: Online Session Agreement (Summary)

For parents and carers, we ask that:

- you are at home, or responsible for your child, during every live session;
- your child joins from a shared space where possible, not a bedroom;
- you do not record or share sessions;
- you let us know straight away if you have any worries about your child's safety or wellbeing.

For young people, we ask that you:

- join sessions using the link sent to your parent or carer;
- are kind and respectful, and dress as you would for an in-person session;
- do not record, screenshot or share the session;
- tell your tutor or a trusted adult if anything online worries you.

Meadow Pathways staff will:

- use only our approved platform and organisation accounts;
- work from a professional space and keep sessions safe and respectful;
- never contact your child outside agreed session times or through personal accounts;
- follow our safeguarding procedures if they have any concern about your child's safety.