

Online Safety Policy

Purpose

PMACTIVE is committed to promoting the safety and wellbeing of children and young people when they use digital technology, the internet, social media and online communication. We recognise that children and young people may use a wide range of online platforms, devices and services as part of their everyday lives. While technology provides many positive opportunities for communication, learning, participation and entertainment, it can also expose children and young people to risks.

This policy sets out how PMACTIVE will promote online safety, reduce risks and respond to concerns involving online activity. This policy applies to all PMACTIVE staff, volunteers, children and young people participating in PMACTIVE activities and, where relevant, parents and carers.

Online Safety and Safeguarding

Online safety is an important part of PMACTIVE's safeguarding responsibilities.

Online activity may create or contribute to safeguarding concerns including:

- Cyberbullying and online harassment.
- Contact from inappropriate or unknown individuals.
- Grooming and exploitation.
- Sexual exploitation or inappropriate sexual contact.
- Sharing or requesting inappropriate images.
- Exposure to harmful, violent or age-inappropriate content.
- Hate speech or discriminatory content.
- Radicalisation or extremist material.
- Online scams, fraud or financial exploitation.
- Pressure, coercion or manipulation.
- Excessive or harmful use of digital technology.
- Risks associated with online gaming, social media or messaging platforms.
- Loss of privacy or inappropriate sharing of personal information.

Where an online concern indicates that a child or young person may be at risk of harm, it will be managed in accordance with PMACTIVE's **Safeguarding Children and Young People Policy**.

Staff and Volunteer Responsibilities

All staff and volunteers have a responsibility to promote safe and appropriate use of technology.

Staff and volunteers must:

- Follow this policy and PMACTIVE's safeguarding procedures.
- Maintain appropriate professional boundaries when communicating online.

- Use approved PMActive systems and communication methods wherever possible.
- Avoid inappropriate or unnecessary contact with children and young people outside agreed PMActive activities.
- Never use online communication to establish secretive or inappropriate relationships with children or young people.
- Never send, request, save or share inappropriate images or content involving children or young people.
- Never use personal social media accounts to communicate privately with children or young people.
- Report online safeguarding concerns promptly to PMActive Management or the Designated Safeguarding Lead (DSL).
- Maintain confidentiality and handle personal information securely.
- Take reasonable steps to prevent children and young people being exposed to inappropriate online content during PMActive activities.

Staff and volunteers must not use their position within PMActive to influence, pressure or manipulate a child or young person online.

Professional Online Communication

Where PMActive needs to communicate with children or young people online, communication should:

- Have a clear and legitimate purpose connected to PMActive activities.
- Take place through an approved communication method wherever possible.
- Be appropriate to the child's age and circumstances.
- Maintain professional boundaries.
- Be transparent and capable of being appropriately monitored or reviewed.
- Avoid unnecessary communication outside agreed hours.

Staff and volunteers should not:

- Use private or disappearing-message functions to communicate with children or young people where this prevents appropriate oversight.
- Engage in inappropriate conversations.
- Share personal photographs or personal information unnecessarily.
- Add children or young people to personal social media accounts.
- Accept or initiate personal social media connections with children or young people.
- Encourage children or young people to keep communications secret from parents, carers or PMActive.

Where a child or young person contacts a member of staff through an inappropriate or personal channel, the staff member should maintain professional boundaries, avoid engaging in inappropriate communication and inform PMActive Management where necessary.

Online Sessions

Where PMACTive provides online or virtual sessions, staff must:

- Use an agreed and appropriate digital platform.
- Obtain appropriate consent before sessions take place.
- Maintain professional boundaries throughout the session.
- Ensure the environment is appropriate and suitable for professional work.
- Avoid unnecessary one-to-one private messaging.
- Follow PMACTive's Lone Working Policy where online work constitutes 1:1 working.
- Ensure safeguarding concerns are reported in the same way as concerns arising during face-to-face activities.

Where appropriate, parents or carers may be informed of the arrangements for online sessions and how they can raise concerns.

PMACTive will not routinely record online sessions unless there is a clear and legitimate reason to do so, appropriate consent has been obtained and the recording is managed securely.

Personal Devices

Staff and volunteers should use PMACTive-approved devices and systems where available.

Where personal devices are used for an authorised operational purpose, staff and volunteers must:

- Use the device responsibly and securely.
- Ensure personal information is protected.
- Avoid storing unnecessary personal information about children and young people.
- Transfer information to an authorised PMACTive system where required.
- Delete information from the personal device as soon as reasonably practicable where appropriate.
- Report any loss, theft, unauthorised access or accidental disclosure immediately to PMACTive Management.

Personal devices must not be used to access, create, store or share inappropriate images or content involving children or young people.

Photography and video are managed in accordance with PMACTive's **Photography, Video and Social Media Policy**.

Social Media

PMACTive recognises that social media can provide positive opportunities for communication, engagement and promotion.

PMACTive's official social media accounts may be used to promote activities, celebrate achievements and share appropriate information about PMACTive.

Content published by PMACTive must be:

- Appropriate and professional.
- Respectful and inclusive.
- Consistent with PMACTive's values.

- In accordance with photography and video consent arrangements.
- Managed in accordance with data protection requirements.

Staff and volunteers must not publish information about children or young people through personal social media accounts. Staff and volunteers must also take care when discussing PMActive or their work on personal social media. Confidential or identifying information about children, young people, families, colleagues or PMActive activities must never be shared.

Photography, Video and Images

PMActive will obtain appropriate consent before taking or using photographs or videos of children and young people for promotional, publicity or other agreed purposes.

Photography and video consent will normally be obtained through the PMActive registration form before a child or young person participates in activities.

Where PMActive receives registration information through third-party booking channels, photography and video consent recorded through those systems will be checked and respected. Consent does not permit staff or volunteers to use images for purposes outside those agreed. Photography and video will be managed in accordance with PMActive's

Photography, Video and Social Media Policy.

Cyberbullying, Bullying and Harassment

PMActive recognises that bullying and harassment may take place online as well as face-to-face.

Online bullying may include:

- Abusive or threatening messages.
- Deliberate exclusion from online groups.
- Sharing embarrassing or harmful content.
- Spreading rumours.
- Creating fake accounts.
- Sharing private information.
- Repeated unwanted contact.
- Sharing images without permission.
- Sexualised or discriminatory messages.

Concerns relating to bullying or harassment will be managed in accordance with PMActive's

Positive Behaviour and Relationships Policy.

Where online bullying or harassment creates a safeguarding concern, PMActive's safeguarding procedures will also apply.

Inappropriate or Harmful Content

PMActive recognises that children and young people may encounter content that is inappropriate, harmful or distressing.

Staff should respond calmly and avoid blaming or shaming the child or young person.

Where a child or young person reports seeing harmful or inappropriate content, staff should:

- Listen and take the concern seriously.
- Reassure the child or young person.
- Avoid unnecessary questioning.
- Report safeguarding concerns to the DSL where appropriate.
- Record the concern where required.
- Follow management or safeguarding guidance regarding any further action.

Staff should not ask a child or young person to forward or share harmful content unless specifically instructed to do so by an appropriate safeguarding or law enforcement professional.

Online Grooming and Exploitation

PMACTive recognises that children and young people may be targeted by individuals seeking to build inappropriate relationships online.

Staff should be alert to concerns such as:

- Secretive online relationships.
- Contact with unknown adults.
- Pressure to move conversations to private platforms.
- Requests for photographs or personal information.
- Offers of gifts, money or other incentives.
- Sexualised conversations or requests.
- Threats, coercion or blackmail.
- Sudden changes in online behaviour or relationships.

Any concern that a child or young person may be experiencing grooming or exploitation must be reported immediately through PMACTive's safeguarding procedures.

Online Radicalisation and Extremism

Children and young people may encounter extremist or radicalising content online.

Concerns relating to radicalisation, extremist influence or terrorism will be managed in accordance with PMACTive's **Prevent and Radicalisation Safeguarding Statement** and Safeguarding Children and Young People Policy. Staff and volunteers should report concerns rather than attempting to investigate or challenge extremist content themselves.

Personal Information and Privacy

Children, young people, parents, carers, staff and volunteers should be encouraged to protect personal information online. PMACTive will not unnecessarily share personal information about children or young people online.

Personal information must be handled in accordance with PMACTive's **Data Protection and Confidentiality Policy** and **Privacy Policy**.

Staff and volunteers must not share information such as:

- Home addresses.

- Personal telephone numbers.
- Personal email addresses.
- Passwords.
- Medical information.
- Confidential family information.
- Information that could identify a child as being in a particular location at a particular time.

Passwords and Cyber Security

Staff and volunteers must take reasonable steps to protect PMActive systems and information.

This includes:

- Using strong passwords.
- Keeping passwords confidential.
- Not sharing account passwords with others.
- Locking devices when unattended.
- Using appropriate security measures.
- Reporting suspected unauthorised access.
- Reporting lost or stolen devices promptly.
- Taking care when opening links or attachments from unknown sources.

Any suspected data breach or loss of personal information must be reported to PMActive Management in accordance with the Data Protection and Confidentiality Policy.

Responding to Online Safeguarding Concerns

Where an online concern is raised, staff and volunteers should:

1. Ensure the immediate safety and wellbeing of the child or young person.
2. Listen calmly and take the concern seriously.
3. Avoid promising secrecy.
4. Avoid unnecessary questioning or investigation.
5. Report the concern to the DSL or PMActive Management without delay.
6. Record the concern factually using the appropriate PMActive recording process.
7. Follow safeguarding advice regarding any further action.

Where there is an immediate risk of serious harm, emergency services or the appropriate safeguarding authority may need to be contacted.

Staff Training and Awareness

PMActive will provide staff and volunteers with appropriate information and training to enable them to understand online safeguarding risks relevant to their role.

Training and awareness may include:

- Online safeguarding risks.
- Cyberbullying.
- Grooming and exploitation.

- Professional boundaries.
- Safe online communication.
- Social media.
- Photography and image sharing.
- Data protection and privacy.
- Radicalisation and extremist content.
- Reporting and responding to safeguarding concerns.

Parents and Carers

PMAActive recognises the important role parents and carers play in supporting children and young people to stay safe online.

Where appropriate, PMAActive may provide information or signposting to help parents and carers understand online risks and support safe use of technology.

Parents and carers are encouraged to raise any online safety concerns with PMAActive.

Staff and Volunteer Conduct

Staff and volunteers must remember that their responsibilities to safeguard children and young people apply both online and offline. Any online conduct that breaches PMAActive's safeguarding expectations, professional boundaries or Code of Conduct may be addressed through PMAActive's relevant procedures. Concerns about the conduct of a staff member or volunteer will be managed in accordance with the **Managing Allegations Against Staff and Volunteers Policy** where appropriate.

Records and Confidentiality

Online safety concerns, incidents and disclosures will be recorded where appropriate and managed securely. Records will be handled in accordance with PMAActive's **Data Protection and Confidentiality Policy** and relevant safeguarding procedures.

Information will only be shared with those who have a legitimate need to know, subject to safeguarding and legal requirements.

Responsibilities

PMAActive Management is responsible for ensuring that appropriate online safety arrangements are in place and that staff and volunteers understand their responsibilities.

The Designated Safeguarding Lead (DSL) is responsible for overseeing safeguarding concerns involving online activity and ensuring that appropriate action is taken.

Staff and volunteers are responsible for following this policy, maintaining professional boundaries and reporting concerns promptly.

Children and young people are encouraged to treat others respectfully online, protect their personal information and tell a trusted adult if something online makes them feel unsafe, worried or uncomfortable.

Parents and carers are encouraged to support children and young people to use technology safely and to raise concerns with PMAActive where appropriate.

Related Policies

This policy should be read alongside:

- Safeguarding Children and Young People Policy.
- Safeguarding Adults Policy.
- Prevent and Radicalisation Safeguarding Statement.
- Photography, Video and Social Media Policy.
- Positive Behaviour and Relationships Policy.
- Equality, Diversity, Inclusion and Anti-Discrimination Policy.
- Data Protection and Confidentiality Policy.
- Privacy Policy.
- Lone Working Policy.
- Staff and Volunteer Code of Conduct.
- Managing Allegations Against Staff and Volunteers Policy.
- Complaints and Compliments Policy.

Review

PMACTive will review this policy regularly and update it where necessary to reflect changes in legislation, safeguarding guidance, technology, online risks and PMACTive's services.

Policy Reviews:

Policy Written: September 2026