beYou Online Safety Policy

Version 1
Completed Date: 15th January 2025
Review Date: 15th January 2026

1. Policy Statement

At beYou, we recognise the importance of ensuring a safe online environment for all children, young people, and staff engaged in our alternative education provision. This policy outlines our approach to promoting online safety and safeguarding individuals from online risks, including cyberbullying, grooming, inappropriate content, and exploitation.

2. Scope

This policy applies to all staff, volunteers, students, and external partners using technology as part of their work with beYou. It covers the use of:

- Internet and email systems.
- Social media platforms.
- Online teaching platforms and communication tools.
- Devices provided by beYou or personal devices used for work-related activities.

3. Key Principles

- Online safety is an integral part of safeguarding.
- Children and young people have a right to access the internet safely.
- Staff must model and promote safe online behaviour.
- All concerns about online safety will be addressed promptly and effectively.

4. Legal Framework

This policy aligns with key legislation and guidance, including:

- *Keeping Children Safe in Education* (KCSIE)
- *Working Together to Safeguard Children*
- The Data Protection Act 2018 and UK GDPR
- The Prevent Duty 2015
- Education Act 2002

5. Roles and Responsibilities

- Designated Safeguarding Lead (DSL): Oversees online safety within the organisation and ensures staff training and compliance.

- Staff and Volunteers: Promote online safety, report concerns, and follow this policy.
- Management Team: Ensure resources and systems are in place to support online safety measures.
- Children and Young People: Follow acceptable use guidelines and report any concerns.

6. Risks of Online Use

Key risks include:

- Cyberbullying: Online harassment, threats, or abuse.
- Inappropriate Content: Exposure to harmful or illegal material, including violence, pornography, and extremism.
- Online Grooming: Manipulation by predators to exploit or harm children.
- Privacy and Data Breaches: Sharing of personal information without consent.
- Radicalisation: Exposure to extremist ideologies.

7. Preventative Measures

- Education and Awareness:
  - All staff and children receive regular training on online safety, including identifying risks and safe practices.
  - Online safety topics are embedded in the curriculum.
- Acceptable Use Policies:
  - All staff and students sign an Acceptable Use Agreement outlining appropriate online behaviour and prohibited activities.
- Supervision and Monitoring:
  - Online activities during sessions are supervised by trained staff.
  - Filters and monitoring software are installed on devices to block harmful content and track inappropriate use.
- Secure Platforms:
  - All online teaching and communication take place on secure, vetted platforms.
  - Strong passwords and two-factor authentication are required for all accounts.
- Data Protection:
  - Personal data is handled in line with GDPR requirements.
  - Staff are trained in secure data management practices.

8. Responding to Concerns

- All online safety concerns must be reported immediately to the DSL.
- Examples of concerns include:
  - A child sharing worrying information about online interactions.
  - Discovery of inappropriate content accessed on organisational devices.
  - Reports of cyberbullying or other harmful online behaviour.
- The DSL will:
  - Record the concern and investigate.
  - Take appropriate action, which may include contacting parents, schools, or external agencies such as the police or social care.
  - Provide support to the affected individual(s).

9. Cyberbullying

- Cyberbullying will not be tolerated. Any reports will be taken seriously and addressed in line with the beYou anti-bullying policy.
- Support will be offered to victims, and disciplinary action may be taken against perpetrators.

10. Training and Development

- Staff and volunteers receive annual online safety training, covering:
  - Recognising online risks.
  - Safe use of technology in educational settings.
  - Reporting procedures for online concerns.

11. Parental Engagement

- beYou works in partnership with parents and carers to promote online safety at home. Resources and workshops may be provided to help parents:
  - Understand online risks.
  - Use parental controls on devices and apps.
  - Encourage open communication with children about their online activities.

12. Monitoring and Review

- This policy will be reviewed annually or sooner if there are significant changes in legislation or technology.
- Feedback from staff, students, and parents will inform updates.

13. Contact Information

- Designated Safeguarding Lead (DSL): Louis Kirk – Co-Founder – louis@firststep-sports.co.uk -
- Deputy DSL: Rob Brown – Managing Director – Robert@firststep-sports.co.uk - 07880231620
- CEOP (Child Exploitation and Online Protection): www.ceop.police.uk
- NSPCC Helpline: 0808 800 5000

Approval and Sign-Off This policy has been approved by the management team and is effective from 15/01/2025.

Signed:
Rob Browm
Managing Director
beYou, First Step Sports Group