Owner and version control

Responsibility:	**Director of Quality & Compliance**	**Date doc. created:**	**20th November 2023**
Print name sign off:	Chris Garcia	**Last review date of doc:**	**April 2026**
Signature:	**Chris Garcia**	**Next review date:**	**March 2027**

Digital and Online Safeguarding Policy (2026–2027)

1. Introduction

This Digital and Online Safeguarding Policy outlines the measures and guidelines implemented by Best Practice Network (BPN) to ensure the safety, security, and well-being of all learners, staff, and stakeholders within our digital and online learning environments.

This policy applies to all BPN digital systems, including learning platforms, communication tools, social media, and third-party applications used for delivery or engagement.

Aligned with relevant UK legislation and statutory guidance, this policy adopts a proactive and preventative approach to safeguarding in the digital space and reflects a whole-organisation approach to safeguarding.

2. Legislative Framework

BPN safeguarding practices comply with and are informed by the following key UK legislation and statutory guidance:

- Children Act 1989 and 2004
- Keeping Children Safe in Education (KCSIE) – latest statutory guidance
- Working Together to Safeguard Children 2023
- Online Safety Act 2023
- Data Protection Act 2018 & UK GDPR
- Counter-Terrorism and Security Act 2015 (Prevent Duty)

This policy reflects statutory expectations and best practice guidance for safeguarding in education, training, and online environments.

3. Roles and Responsibilities

Designated Safeguarding Lead (DSL)

- Oversees all aspects of online safeguarding
- Ensures compliance with legislation and best practice
- Manages safeguarding incidents and referrals

Deputy DSL(s)

- Supports the DSL and acts in their absence

Teaching and Support Staff

- Promote safe and responsible online behaviour
- Identify and respond to safeguarding risks
- Record and report concerns promptly in line with BPN procedures

All staff have a duty to report safeguarding concerns immediately and no later than the same working day.

IT and Digital Teams

- Maintain secure systems and platforms
- Implement filtering, monitoring, and access controls
- Support incident response relating to digital risks

Learners

- Are expected to engage responsibly in digital environments
- Are supported to develop awareness of online safety risks through training and resources (e.g. UK Safer Internet Centre)

---

4. Online Safety Measures

To mitigate risks, BPN implements the following controls:

Technical Safeguards

- Internet filtering and monitoring systems to restrict harmful or inappropriate content
- Secure user authentication aligned with National Cyber Security Centre (NCSC) guidance
- Encrypted communication and data handling in line with ICO standards

Platform Governance

- All digital platforms used for delivery must be risk-assessed and approved prior to use
- Third-party tools must meet safeguarding and data protection requirements

Behaviour and Conduct

- Clear expectations for professional conduct and communication are maintained at all times
- Staff must maintain appropriate boundaries when interacting with learners online

Emerging Risks and Technologies

- The use of artificial intelligence (AI) tools is monitored to prevent misuse, including impersonation, inappropriate content generation, or safeguarding breaches
- Risks associated with social media, messaging platforms, and emerging technologies are actively monitored and managed

---

5. Reporting and Responding to Incidents

All safeguarding concerns must be reported immediately to the Designated Safeguarding Lead (DSL) via **safeguarding@bestpracticenet.co.uk**.

Concerns must be reported as soon as possible and no later than the same working day.

All incidents must be recorded in accordance with BPN safeguarding procedures.

Types of Concerns

Incidents may include (but are not limited to):

- Online abuse or harassment
- Inappropriate communication or contact
- Cyberbullying
- Radicalisation or extremism concerns
- Exploitation or grooming risks
- Data breaches impacting safeguarding

Response and Support

- All concerns are assessed and escalated in line with KCSIE and statutory guidance
- Appropriate support and intervention are provided to affected individuals
- External agencies (e.g. NSPCC, local safeguarding partnerships) are engaged where required

---

6. Acceptable Use and Digital Conduct

All users must adhere to BPN's acceptable use expectations, including:

- Use of authorised platforms only
- Maintaining professional and appropriate communication
- Respecting privacy, confidentiality, and data protection requirements
- Not engaging in behaviour that could place themselves or others at risk

Breaches of acceptable use may result in disciplinary action.

---

7. Policy Review

This policy is reviewed annually to ensure compliance with evolving legislation and best practice.

It will also be reviewed following any significant safeguarding incident, legislative update, or identified emerging risk.

Updates will be communicated to all relevant stakeholders.

---

8. Conclusion

Best Practice Network is committed to fostering a secure, inclusive, and responsible digital learning environment. Through this policy, we uphold the highest standards of online safeguarding, enabling all members of our community to engage safely and confidently in digital spaces.