



Bouncing Statistics

Overcoming the misunderstood conception

Lead member of staff and DSL: Ryan Blackwood

Version: 2.0 |

Review date: Sept 2027

Checked date: 02/09/2026

First amendment date: 30/07/2025

Section 1 – Introduction and Scope

Staff must use C-017 – Online Safety Concern Flowchart alongside SOP-002 – Reporting a Safeguarding Concern and C-004 – DSL Decision-Making & Thresholds, where applicable. Where an online safety concern relates to the DSL, it must be escalated through the appropriate senior leadership or Board route and must not be managed by the DSL concerned. Online safety forms part of the organisation's wider safeguarding arrangements. The DSL provides strategic oversight and day-to-day safeguarding leadership. The Deputy DSL provides support and safeguarding cover.

Deputy DSL: Joel Ambalu

Policy owner: Designated Safeguarding Lead (DSL) – Ryan Blackwood

Policy Ownership and Key Contacts

1.1 Statement of Commitment

Bouncing Statistics CIC recognises that digital technology plays a fundamental role in the education, development and everyday lives of children and young people. While technology provides significant opportunities for learning, communication, creativity and personal development, it also presents safeguarding risks that require effective leadership, education and robust safeguarding arrangements.

We are committed to creating an environment where children, young people and staff can use digital technologies safely, responsibly and confidently. Online safety is recognised as an integral part of safeguarding and child protection and is embedded within our wider safeguarding culture rather than being viewed as a separate responsibility.

Our approach to online safety is child-centred, trauma-informed and strengths-based. We recognise that children accessing our provision may have experienced online harm, exploitation, cyberbullying or other digital safeguarding concerns. We are committed to responding to these concerns with professional curiosity, appropriate intervention and partnership working, while empowering children to develop the knowledge, skills and resilience needed to navigate the online world safely.

Effective online safeguarding requires the shared responsibility of staff, children, parents, carers and partner agencies. Through education, clear expectations, appropriate filtering and monitoring, professional practice and continuous improvement, Bouncing Statistics aims to foster a positive digital culture where technology is used safely, ethically and to enhance learning and wellbeing.

1.2 Purpose

I would add a dedicated purpose section, which your safeguarding policy doesn't explicitly have.

The purpose of this policy is to:

- Promote the safe, responsible and effective use of digital technologies across Bouncing Statistics.
- Protect children, young people and staff from online harm.
- Establish clear expectations for the use of digital devices, online platforms and social media.
- Support staff in recognising, responding to and recording online safeguarding concerns.
- Ensure compliance with current legislation and statutory guidance.
- Promote a culture of digital responsibility, respect and resilience.

1.3 Scope

Exactly the same wording style as your safeguarding policy.

This policy applies to:

- All employees
- Volunteers
- Agency staff

- Contractors
- Visitors
- Trustees and Directors
- Students on placement
- External professionals working on behalf of Bouncing Statistics

The policy applies across all services delivered by Bouncing Statistics, including:

- Eden House Alternative Provision
- Inclusion Hubs
- One-to-one mentoring
- School outreach
- Holiday programmes
- Community-based interventions
- Off-site educational activities
- Online and remote learning

Any digital platform or technology used to support the organisation's work

1.4 Relationship with the Safeguarding & Child Protection Policy

This policy should be read alongside the Bouncing Statistics Safeguarding & Child Protection Policy. Where an online safety concern places a child at risk of harm, or where abuse, exploitation or criminal activity is suspected, it will be managed in accordance with the organisation's safeguarding procedures. Online safety concerns will be recorded, assessed and responded to using the same safeguarding principles, reporting arrangements and decision-making processes outlined within the Safeguarding & Child Protection Policy.

Section 2 – Legislative and Regulatory Framework

2.1 Legislative and Statutory Framework

Bouncing Statistics is committed to ensuring that its online safety arrangements reflect current legislation, statutory guidance and recognised best practice. This policy has been developed to support the organisation's wider safeguarding responsibilities and should be read alongside the Safeguarding & Child Protection Policy and other related safeguarding procedures.

The organisation recognises that online safety is a safeguarding responsibility and that digital risks should be managed using the same child-centred approach applied to all safeguarding concerns.

This policy is informed by, but not limited to, the following legislation and statutory guidance:

- Keeping Children Safe in Education (KCSIE) 2026
- Working Together to Safeguard Children 2026
- Online Safety Act 2023
- Children Act 1989
- Children Act 2004
- Education Act 2002
- Data Protection Act 2018
- UK General Data Protection Regulation (UK GDPR)
- Human Rights Act 1998
- Equality Act 2010
- Prevent Duty Guidance
- UK Council for Internet Safety (UKCIS) guidance
- ICO Children's Code (Age Appropriate Design Code)
- Appropriate Filtering and Monitoring Standards for Schools and Colleges
- Local Safeguarding Children Partnership procedures

The organisation will review this policy whenever there are significant changes to legislation, statutory guidance or emerging online safeguarding risks to ensure that practice remains effective, lawful and responsive.

2.2 Our Regulatory Commitment

Bouncing Statistics recognises that effective online safety extends beyond legal compliance. The organisation is committed to creating a digital culture where safeguarding, education and responsible technology use are embedded throughout daily practice.

To achieve this, we will:

- maintain robust safeguarding arrangements for all online activity
- ensure that online safety is integrated into safeguarding, behaviour and curriculum planning
- promote safe, responsible and ethical use of technology
- implement appropriate filtering and monitoring systems
- educate children and young people about online risks and digital resilience
- provide staff with regular training and safeguarding updates
- work collaboratively with parents, carers, commissioning schools and partner agencies
- regularly review online safety arrangements through quality assurance and continuous improvement.

2.3 Emerging Technologies

Bouncing Statistics recognises that digital technology continues to evolve rapidly and that safeguarding arrangements must evolve accordingly.

The organisation will regularly review the impact of emerging technologies, including:

- Artificial Intelligence (AI)
- Generative AI platforms
- Deepfake technology
- Virtual and augmented reality
- Live-streaming platforms
- Social media developments
- Gaming platforms
- Encrypted messaging applications
- New and emerging digital communication technologies.

Where new risks are identified, the organisation will review procedures, provide appropriate staff guidance and update this policy where necessary to ensure that safeguarding arrangements remain effective.

Section 3 – Digital Safeguarding Ethos and Principles

3.1 Our Digital Safeguarding Ethos

At Bouncing Statistics, online safety is not viewed solely as the management of technology or internet access. It is recognised as a fundamental safeguarding responsibility that underpins the welfare, wellbeing and development of every child and young person.

We recognise that digital technology is an integral part of modern life and education. Children use online platforms to learn, communicate, socialise, create and access information. While these opportunities can enhance learning and personal development, they also introduce safeguarding risks that require education, vigilance and appropriate professional oversight.

Our approach to digital safeguarding is proactive rather than reactive. We seek to create a culture where children develop the knowledge, confidence and resilience to use technology safely and responsibly, while ensuring that staff have the skills and confidence to identify, respond to and record online safeguarding concerns effectively.

Online safety is embedded throughout our safeguarding culture and is reflected in our policies, procedures, staff training, curriculum delivery and day-to-day practice. Every member of staff shares responsibility for promoting safe digital behaviours and protecting children from online harm.

We recognise that effective online safeguarding is achieved through education, positive relationships, clear expectations, professional curiosity and collaborative working with children, families, commissioning schools and safeguarding partners.

3.2 Our Digital Safeguarding Principles

Our approach to online safety is underpinned by the following principles.

Child-Centred Practice

The welfare of the child remains the paramount consideration in all online safeguarding decisions.

Children will be supported to develop the knowledge, confidence and resilience to use technology safely while recognising that their individual needs, experiences and vulnerabilities may influence how they engage with digital environments.

Education Before Restriction

We believe that teaching children how to use technology safely is more effective than relying solely on restrictions.

Children will be supported to understand:

- safe online behaviour
- respectful digital communication
- privacy and personal information
- recognising online risks
- reporting concerns
- responsible use of emerging technologies

Where restrictions are necessary to reduce safeguarding risks, these will be proportionate and balanced with opportunities for learning and personal development.

Trauma-Informed Practice

We recognise that children accessing our provision may have experienced online abuse, exploitation, cyberbullying or other harmful digital experiences.

Staff will respond with empathy, professional curiosity and appropriate safeguarding interventions while maintaining high expectations for safe and respectful online behaviour.

Digital behaviour will always be considered within the wider context of the child's experiences, wellbeing and safeguarding needs.

Professional Curiosity

Online safeguarding concerns are not always immediately visible.

Staff are expected to remain professionally curious where they identify changes in a child's behaviour, emotional wellbeing, technology use or online interactions that may indicate abuse, exploitation or other safeguarding concerns.

Staff should never assume that online incidents are isolated or insignificant without appropriate consideration and discussion with the Designated Safeguarding Lead (DSL).

Digital Citizenship

Bouncing Statistics is committed to promoting responsible, respectful and ethical use of technology.

Children will be encouraged to become positive digital citizens by:

- treating others with respect online
- recognising the impact of their digital behaviour
- understanding consent and privacy
- using technology responsibly
- challenging harmful online behaviour where it is safe to do so

Partnership Working

Online safeguarding is most effective when organisations, families and partner agencies work collaboratively.

Bouncing Statistics will work closely with:

- children and young people

- parents and carers
- commissioning schools
- local authorities
- safeguarding partners
- technology providers where appropriate
- law enforcement agencies where necessary

Information will be shared lawfully, proportionately and in the best interests of the child.

Continuous Improvement

Technology evolves rapidly, and so must our safeguarding practice.

Bouncing Statistics is committed to continually reviewing:

- emerging technologies
- online safeguarding risks
- organisational procedures
- staff training
- filtering and monitoring arrangements
- lessons learned from safeguarding incidents
- national guidance and best practice

Continuous improvement ensures that our online safeguarding arrangements remain effective, proportionate and responsive to the changing digital landscape.

3.3 Digital Safeguarding in Practice

To ensure that online safety remains embedded throughout the organisation, Bouncing Statistics will:

- promote a culture where online safety is everyone's responsibility
- educate children to use technology safely, responsibly and respectfully
- implement appropriate filtering, monitoring and cyber security measures
- ensure online safeguarding concerns are recorded promptly using CPOMS
- respond to online safeguarding concerns in a timely and proportionate manner
- support staff through regular safeguarding and online safety training
- work collaboratively with families, commissioning schools and partner agencies
- regularly review digital safeguarding arrangements through quality assurance activities

Section 4 – Roles and Responsibilities

4.1 Shared Responsibility

Online safety is a shared responsibility. Every member of the Bouncing Statistics community has a role in creating and maintaining a safe digital environment for children and young people.

Whilst the Designated Safeguarding Lead (DSL) provides strategic leadership for online safety, all staff are responsible for promoting safe digital practices, recognising online safeguarding concerns and responding appropriately in accordance with this policy and the organisation's safeguarding procedures.

4.2 Directors

The Directors are responsible for ensuring that:

- online safety is embedded within the organisation's safeguarding arrangements
- appropriate policies, procedures and resources are in place
- statutory safeguarding responsibilities relating to online safety are fulfilled
- appropriate filtering and monitoring arrangements are implemented where required
- sufficient resources are available to support staff training and technological safeguards
- online safety is monitored through governance, quality assurance and policy review

4.3 Designated Safeguarding Lead (DSL)

The DSL has strategic responsibility for leading and overseeing online safety across the organisation.

This includes:

- ensuring that online safety is fully integrated within safeguarding practice;
- providing advice, guidance and support to staff regarding online safeguarding concerns
- receiving and reviewing concerns relating to online abuse, exploitation or harmful online behaviour
- ensuring appropriate referrals are made where safeguarding thresholds are met;
- monitoring trends and emerging online safeguarding risks
- ensuring concerns are accurately recorded on CPOMS
- working with commissioning schools, families and external agencies where appropriate
- ensuring online safety forms part of staff induction and ongoing safeguarding training
- reviewing the effectiveness of this policy and recommending improvements where required

4.4 Deputy Designated Safeguarding Lead (DDSL)

The Deputy DSL will:

- support the DSL in implementing this policy
- fulfil the responsibilities of the DSL when delegated or during periods of absence
- assist in monitoring online safeguarding concerns
- contribute to staff guidance, safeguarding reviews and quality assurance activities

4.5 Managers

Managers are responsible for:

- promoting compliance with this policy within their areas of responsibility
- modelling safe and professional use of technology
- supporting staff to follow organisational procedures
- escalating safeguarding concerns without delay
- identifying any training or support needs within their teams
- contributing to quality assurance and continuous improvement

4.6 Staff, Volunteers and Placement Students

Every adult working on behalf of Bouncing Statistics has a responsibility to:

- safeguard children from online harm
- maintain appropriate professional boundaries when using technology
- use organisational technology responsibly and securely
- follow all organisational policies relating to online safety and safeguarding
- immediately report any online safeguarding concern to the DSL or Deputy DSL
- accurately record concerns using CPOMS
- participate in mandatory safeguarding and online safety training
- challenge inappropriate digital behaviour where safe and appropriate to do so
- protect confidential information and personal data

No member of staff should ignore, minimise or delay reporting concerns because they believe another person may have already acted.

4.7 Children and Young People

Children and young people accessing Bouncing Statistics are encouraged to:

- use technology safely and respectfully
- treat others with kindness and respect online
- protect their own personal information
- report anything online that makes them feel unsafe, uncomfortable or worried
- follow staff guidance regarding the use of digital devices and online platforms
- contribute positively to creating a safe digital environment

Children will never be blamed for reporting online concerns and will be supported appropriately where risks are identified.

4.8 Parents, Carers and Commissioning Schools

Bouncing Statistics recognises that effective online safety is strengthened through partnership working.

Parents, carers and commissioning schools are encouraged to:

- support safe technology use beyond the educational setting;
- share relevant safeguarding information where appropriate;
- communicate concerns regarding online safety promptly;
- work collaboratively with the organisation to safeguard children and young people.

Where concerns meet safeguarding thresholds, information will be shared in accordance with safeguarding procedures and relevant data protection legislation.

4.9 External Professionals and Partner Agencies

Where external professionals deliver services on behalf of Bouncing Statistics, they are expected to:

- comply with this policy and related safeguarding procedures
- maintain appropriate professional boundaries
- report safeguarding concerns without delay
- cooperate with safeguarding enquiries and investigations where required
- adhere to relevant confidentiality and information-sharing requirements

Section 5 – Safe Use of Technology

5.1 Purpose

Technology is an integral part of education, communication and service delivery at Bouncing Statistics. This section establishes the standards and expectations for the safe, responsible and professional use of digital technologies by staff, volunteers, children, young people and others working on behalf of the organisation.

The aim is to maximise the educational and operational benefits of technology while reducing safeguarding, security and reputational risks.

5.2 Acceptable Use

All users are expected to use technology in a lawful, respectful and professional manner.

Technology should only be used to:

- support learning and positive outcomes
- communicate professionally
- undertake organisational duties
- access approved educational resources
- record and manage information appropriately
- support safeguarding and wellbeing

Technology must not be used to:

- access illegal or inappropriate material
- harass, intimidate or discriminate against others
- compromise safeguarding
- breach confidentiality
- damage the reputation of Bouncing Statistics
- bypass organisational security measures

5.3 Organisational Devices

Where organisational devices are provided, users must:

- keep devices secure
- lock devices when unattended
- protect passwords
- install updates when required
- report damage, loss or theft immediately
- avoid installing unauthorised software

5.4 Personal Devices (BYOD)

Where personal devices are used for organisational purposes, staff must ensure that:

- devices are password protected
- organisational information is stored securely

- confidential information is not retained unnecessarily
- approved communication methods are used
- any compromise of information is reported immediately

The use of personal devices by children and young people will be managed through local procedures, individual risk assessments and the Behaviour Policy.

5.5 Artificial Intelligence (AI)

Bouncing Statistics recognises that Artificial Intelligence has an increasing role within education and professional practice.

AI may be used to support planning, administration and learning where its use is:

- ethical
- proportionate
- professionally reviewed
- compliant with data protection requirements

Staff must not:

- upload confidential information into public AI systems
- rely solely on AI when making safeguarding decisions
- present AI-generated content as verified without checking its accuracy

Children may be introduced to AI in an age-appropriate, supervised manner to promote digital literacy and critical thinking.

5.6 Digital Communication

All digital communication should remain professional, respectful and appropriate.

Staff must:

- maintain professional boundaries
- use approved communication channels
- avoid personal messaging with children or young people
- communicate respectfully
- protect confidential information

5.7 Social Media

Staff should use social media responsibly and maintain appropriate professional boundaries.

Personal social media accounts must not be used to communicate with children attending Bouncing Statistics.

Staff should be mindful that their online activity may impact public confidence in the organisation.

5.8 Remote Learning and Digital Platforms

Where digital platforms are used to deliver education or intervention:

- approved platforms should be used
- safeguarding expectations remain unchanged
- professional standards apply at all times
- concerns arising during online sessions must be managed in accordance with safeguarding procedures

Section 6 – Online Risks and Safeguarding Responses

Where Bouncing Statistics operates within a commissioning school or other host setting, staff will follow the host setting's reasonable device, filtering and acceptable-use arrangements alongside Bouncing Statistics safeguarding procedures.

Where a device is believed to contain material relevant to a safeguarding concern, staff must not search it themselves unless they are specifically authorised and the action is lawful and proportionate. The matter should be escalated to the DSL and, where appropriate, the relevant host setting or statutory agency.

Personal mobile phones and other personal devices must be used in accordance with local setting rules, individual risk assessments and organisational safeguarding expectations. Staff must not use

personal devices to photograph, record or privately message children unless there is a specific, authorised organisational process that permits this.

Bouncing Statistics will maintain clear acceptable-use expectations for staff, children and other users of organisational technology. These expectations will be communicated through induction, safeguarding training, relevant agreements and local procedures.

5.9 Acceptable Use and Mobile Devices

6.1 Understanding Online Risks

Children and young people may encounter online risks through social media, messaging applications, gaming, livestreaming, search engines, websites, digital learning platforms, artificial intelligence and other emerging technologies. Online harm may occur alongside offline harm and may affect welfare, behaviour, attendance, relationships and engagement with education.

Bouncing Statistics recognises four broad categories of online risk:

Content – exposure to illegal, harmful or inappropriate material, including pornography, violent or graphic content, hate or discriminatory material, extremist or radicalising content, misinformation, self-harm or suicide content, and other material unsuitable for the child.

Contact – harmful interaction with another person, including grooming, exploitation, coercion, harassment, manipulation, peer pressure or contact from an adult or unknown individual.

Conduct – behaviour by a child or adult that creates or increases risk, including cyberbullying, harassment, sharing inappropriate or intimate images, impersonation, misuse of accounts, discriminatory behaviour and harmful use of AI.

Commerce – financial or commercial exploitation, including scams, phishing, gambling, inappropriate advertising, in-app purchasing pressure and misuse of personal information.

6.2 Online Abuse, Exploitation and Grooming

Online abuse and exploitation may include child sexual abuse, child sexual exploitation, child criminal exploitation, grooming, sextortion, coercive or controlling behaviour, trafficking, radicalisation, peer-on-peer abuse facilitated through technology and image-based abuse.

Staff should remain professionally curious where a child's online behaviour, relationships, access to devices, emotional presentation or patterns of communication indicate a possible safeguarding concern. Concerns must be reported to the DSL/DDSL without unnecessary delay.

6.3 Nudes, Semi-Nudes and AI-Generated Sexual Imagery

Any concern involving nude or semi-nude images of a child, requests for such images, threats to share images, sextortion or sexualised AI-generated imagery must be treated as a safeguarding concern.

Staff must not copy, forward, download, store or share sexual images of children and must not investigate the circumstances independently. The DSL will determine the appropriate safeguarding response and whether external agencies need to be involved.

Where appropriate, children may be supported to use recognised reporting and removal services such as Childline's Report Remove service, alongside safeguarding support.

6.4 Harmful Content, Self-Harm and Suicide

Children may encounter content that promotes or normalises self-harm, suicide, eating disorders, violence, hatred, extremism, pornography or other harmful behaviour. Exposure should be considered in the context of the child's age, understanding, vulnerabilities and wider safeguarding circumstances. Any indication that online content is contributing to immediate risk, self-harm, suicidal thoughts, exploitation or significant emotional distress must be escalated through safeguarding procedures without delay.

6.5 Cyberbullying and Online Peer Abuse

Cyberbullying may include abusive or threatening messages, harassment, exclusion from online groups, spreading rumours, impersonation, sharing humiliating images or videos, trolling, discriminatory abuse or AI-generated content used to intimidate or humiliate.

Staff should not dismiss harmful online behaviour as 'banter'. Responses should consider the safety and welfare of the child affected, the behaviour and circumstances of the child responsible, witnesses and the wider peer context. Responses may include safeguarding action, restorative work, behaviour support, risk assessment, parental engagement and ongoing monitoring.

6.6 Online Gaming, Livestreaming and Social Media

Online gaming, livestreaming and social media can provide positive opportunities for communication and learning but may also expose children to grooming, bullying, harmful content, financial exploitation, inappropriate contact, pressure to share personal information and other safeguarding risks.

Staff should remain professionally curious and avoid assumptions about a child's online activity. Where a concern is identified, the matter should be discussed with the DSL/DDSL and managed through the appropriate safeguarding route.

6.7 Radicalisation and Extremism

Children may encounter extremist or radicalising content online. Any concern that a child may be being influenced, manipulated or drawn towards extremist ideology must be reported to the DSL and managed in accordance with Prevent and safeguarding arrangements. Immediate risks of serious harm must be treated as an emergency.

6.8 Artificial Intelligence, Deepfakes and Emerging Technologies

Generative AI, deepfakes, synthetic media and AI chatbots create both educational opportunities and new safeguarding risks. These may include fabricated evidence, impersonation, AI-generated abuse, sexualised imagery, harassment, misinformation, manipulation, privacy breaches and unsafe or harmful advice.

Staff must treat AI-generated abuse or harmful content as a safeguarding matter, report concerns promptly and never rely solely on AI-generated information when making safeguarding decisions. Staff remain professionally responsible for work produced using AI.

Children will be supported to develop age-appropriate digital literacy, including questioning whether online content is genuine, recognising manipulated media, protecting personal information and knowing how to report concerns.

6.9 Responding to an Online Safety Concern

When an online safety concern is identified, staff must follow C-017 – Online Safety Concern Flowchart and the wider safeguarding procedures.

Immediate response should include:

1. Consider whether the child is at immediate risk of significant harm and take immediate protective action where necessary.
2. Contact 999 where there is an immediate emergency requiring police, ambulance or other emergency assistance.
3. Preserve relevant information or evidence where it is safe and appropriate to do so.
4. Report the concern immediately to the DSL or DDSL; verbal reporting should be used where appropriate so urgent concerns are not delayed by recording.
5. Record the concern factually on CPOMS as soon as possible, following SOP-003 – CPOMS Recording Standards.
6. Do not conduct an independent investigation, confront alleged perpetrators or access another person's account without appropriate authority.
7. The DSL/DDSL will assess the concern and determine the next safeguarding action using SOP-004/C-004 – DSL Decision-Making & Thresholds.

Where the concern involves serious harm, exploitation, abuse, criminal activity or significant risk, the DSL will consider referral or consultation with Children's Social Care, Police, the commissioning school, the Local Authority, Prevent or another relevant safeguarding partner as appropriate.

6.10 Supporting Children After an Online Incident

Online safety responses should be proportionate, child-centred and educational. Support may include reassurance, digital safety education, restorative work, parental/carers engagement, targeted intervention, an individual risk assessment, safeguarding support or referral to specialist agencies. Children will not be blamed for reporting online concerns. Their wishes and feelings, age, understanding, vulnerabilities and wider circumstances will be considered when determining the response.

Section 8 – Filtering, Monitoring and Cyber Security

8.1 Purpose

Bouncing Statistics recognises that effective online safety requires both education and appropriate technical safeguards. Filtering, monitoring and cyber security arrangements help reduce the risk of

children, young people and staff being exposed to harmful or inappropriate online content while supporting the safe and effective use of digital technologies.

Technical measures are intended to support, rather than replace, professional vigilance. Filtering and monitoring systems cannot identify every safeguarding concern and do not remove the responsibility of staff to remain alert to signs of online harm.

8.2 Filtering Arrangements

Where internet-enabled devices or networks are provided by Bouncing Statistics, appropriate filtering measures will be implemented to reduce access to illegal, harmful or inappropriate online content.

Filtering arrangements should, where appropriate:

- prevent access to illegal content
- reduce access to inappropriate or harmful material
- support age-appropriate internet use
- balance safeguarding with legitimate educational access
- be reviewed periodically to ensure they remain effective

Where internet access is provided through a commissioning school or third-party venue, Bouncing Statistics will work collaboratively with the host organisation to understand and follow the relevant filtering arrangements.

8.3 Monitoring Arrangements

Filtering and monitoring arrangements will be reviewed when significant changes occur, including the introduction of new platforms, generative AI tools, image-generation services, changes in service delivery or emerging online safeguarding risks.

Filtering and monitoring should reduce safeguarding risk without creating unreasonable barriers to legitimate teaching, learning, accessibility or professional activity. Where Bouncing Statistics uses a host school's or commissioning organisation's network, the organisation will work with that setting to understand how filtering and monitoring operate and how safeguarding alerts are escalated.

8.3A Proportionate Filtering and Monitoring

Monitoring arrangements are designed to identify behaviours or activity that may indicate safeguarding concerns, misuse of technology or breaches of organisational policy.

Monitoring may include:

- inappropriate internet searches
- attempts to access restricted material
- cyber security alerts
- misuse of organisational devices
- safeguarding concerns identified during online learning or digital activities

Monitoring is undertaken to support safeguarding, organisational security and professional accountability. It is not intended to unnecessarily monitor personal activity or create a culture of surveillance.

8.4 Cyber Security

All staff share responsibility for protecting organisational systems, information and digital resources.

Staff are expected to:

- protect usernames and passwords
- use multi-factor authentication where available
- keep devices updated
- avoid downloading unauthorised software
- verify emails before opening attachments or links
- report suspected phishing or cyber attacks immediately
- securely store and dispose of sensitive information

Any suspected cyber security incident should be reported to a manager and the Designated Safeguarding Lead where there may be safeguarding implications.

8.5 Data Protection and Confidential Information

Children's personal information must be handled securely and in accordance with the organisation's Data Protection Policy and applicable legislation.

Staff must:

- only access information necessary for their role
- store information securely
- share information on a need-to-know basis
- use approved systems for safeguarding records
- ensure confidential information is not visible to unauthorised individuals;
- report any actual or suspected data breach immediately.

The protection of personal information forms an essential part of safeguarding practice.

8.6 Digital Safeguarding During Off-Site and Remote Activities

Where digital technology is used during outreach, educational visits, home-based interventions or remote learning, staff must ensure that safeguarding arrangements remain effective.

This includes:

- using approved platforms where possible
- maintaining professional boundaries
- considering privacy and confidentiality
- following lone working procedures where applicable

reporting any safeguarding concerns in accordance with organisational procedures.

Safeguarding expectations remain the same regardless of where digital interactions take place.

8.7 Reviewing Technical Safeguards

Bouncing Statistics will periodically review its filtering, monitoring and cyber security arrangements to ensure they remain appropriate to the organisation's size, services and operational needs.

Reviews may consider:

- emerging safeguarding risks
- changes in technology
- feedback from staff
- safeguarding incidents and lessons learned
- updates to statutory guidance
- changes to organisational systems or digital platforms

Where improvements are identified, appropriate action will be taken to strengthen safeguarding arrangements.

Section 9 – Recording, Reporting and Managing Online Safety Concerns

9.1 Reporting Concerns

All online safety concerns must be taken seriously and responded to promptly.

Any member of staff who becomes aware of behaviour, communication or online activity that places a child or young person at risk, or may indicate abuse, exploitation or another safeguarding concern, must report this immediately to the Designated Safeguarding Lead (DSL) or Deputy DSL.

Staff should never assume that another colleague has reported a concern or delay reporting while gathering additional information.

Where a child is believed to be at immediate risk of harm, staff must follow the organisation's emergency safeguarding procedures without delay.

9.2 Recording Concerns

All online safeguarding concerns must be recorded accurately, factually and as soon as reasonably practicable using the organisation's safeguarding recording system (CPOMS).

Records should include, where appropriate:

- the date and time of the concern
- a factual account of what was seen, heard or disclosed
- the names of those involved
- any action taken to safeguard the child
- details of any evidence that has been preserved
- any immediate decisions or referrals made
- Staff should avoid including personal opinions or assumptions and should record only factual information.

Further guidance is available within SOP-003 – CPOMS Recording Standards.

9.3 Preserving Digital Evidence

Where an online safety concern involves digital content or communications, reasonable steps should be taken to preserve evidence without placing the child or member of staff at further risk.

Examples may include:

- retaining screenshots where appropriate
- preserving URLs or website details
- recording usernames or account information
- noting the date, time and platform involved

Staff must not:

- conduct their own investigation
- access accounts without appropriate authority
- forward indecent images or unlawful material
- delete evidence unless advised by the Designated Safeguarding Lead or relevant authorities.

Where indecent images of a child are involved, staff must follow statutory guidance and immediately consult the DSL.

9.4 Responding to Concerns

The Designated Safeguarding Lead (DSL) will assess each concern on its individual merits and determine the most appropriate course of action.

This may include:

providing advice or guidance;

- speaking with the child
- engaging parents or carers where appropriate
- implementing safeguarding measures
- completing an individual risk assessment
- making referrals to external agencies
- consulting with the commissioning school
- reporting criminal matters to the police where required

All decisions will be made in the best interests of the child, taking account of their wishes, age, understanding and individual circumstances.

9.5 Information Sharing

Information relating to online safety concerns will be shared lawfully, proportionately and on a need-to-know basis.

Information may be shared where necessary to:

- safeguard a child or young person
- support multi-agency working
- comply with legal or statutory duties
- protect others from harm

All information sharing will be undertaken in accordance with:

- the Safeguarding & Child Protection Policy
- the Data Protection Policy
- UK GDPR
- the Data Protection Act 2018

9.6 Learning from Incidents

Bouncing Statistics is committed to learning from online safety incidents to strengthen safeguarding practice.

Where appropriate, incidents may be reviewed to:

- identify patterns or emerging risks
- improve organisational procedures
- inform staff training
- strengthen preventative education
- enhance risk assessments
- support continuous improvement

Learning from incidents contributes to the organisation's wider safeguarding quality assurance arrangements.

9.7 Links to Safeguarding Procedures

This policy should be read alongside the following organisational procedures:

- Safeguarding & Child Protection Policy
- SOP-001 – Responding to a Safeguarding Disclosure
- SOP-002 – Reporting a Safeguarding Concern
- SOP-003 – CPOMS Recording Standards
- SOP-004 – DSL Decision-Making Framework
- Safeguarding Action Tracker
- Information Sharing Procedures

Where there is any uncertainty regarding the management of an online safety concern, staff must seek advice from the Designated Safeguarding Lead (DSL).

Section 10 – Training, Awareness and Education

10.1 Commitment to Training

Bouncing Statistics recognises that effective online safety depends upon knowledgeable, confident and well-supported staff. Online safety training forms an integral part of the organisation's wider safeguarding training programme and is essential in maintaining a safe digital environment for children, young people and staff.

All staff are expected to understand their responsibilities under this policy and to apply safe digital practices within their day-to-day roles.

10.2 Staff Training

All staff, volunteers and individuals working on behalf of Bouncing Statistics will receive appropriate online safety training that is proportionate to their role and responsibilities.

Training may include:

- recognising online safeguarding risks
- identifying indicators of online abuse and exploitation
- responding to online safety concerns
- recording concerns using CPOMS
- professional use of technology and digital communication
- cyber security awareness
- data protection and confidentiality
- emerging technologies, including Artificial Intelligence (AI)
- updates to legislation, statutory guidance and organisational procedures

Online safety will also form part of the organisation's induction programme for all new staff.

10.3 Ongoing Professional Development

Online safety is an evolving area of safeguarding practice. To ensure staff remain informed and confident, Bouncing Statistics will provide opportunities for continued professional development.

This may include:

- safeguarding updates
- briefings on emerging online risks
- annual refresher training
- lessons learned from safeguarding reviews
- updates following changes in legislation or national guidance
- external training opportunities where appropriate

Staff are encouraged to seek advice from the Designated Safeguarding Lead (DSL) whenever they are uncertain about any aspect of online safety.

10.4 Education for Children and Young People

Bouncing Statistics is committed to developing the digital knowledge, skills and resilience of children and young people.

Where appropriate, online safety education will be integrated into the curriculum, mentoring sessions and wider pastoral support. Topics may include:

- staying safe online
- protecting personal information
- respectful online communication
- recognising online manipulation and exploitation
- responsible use of social media
- cyberbullying
- digital wellbeing
- Artificial Intelligence and critical thinking
- reporting concerns and seeking help

Learning will be age-appropriate, inclusive and responsive to the needs of individual learners.

10.5 Working with Parents, Carers and Partner Organisations

Bouncing Statistics values the role of parents, carers and partner organisations in promoting online safety.

Where appropriate, the organisation will:

- provide advice and guidance to families
- encourage open communication regarding online safety concerns
- work collaboratively with commissioning schools and safeguarding partners
- signpost families to trusted sources of information and support

Effective partnership working strengthens the safeguarding of children both within and beyond the organisation.

10.6 Promoting a Positive Digital Culture

Beyond formal training, Bouncing Statistics aims to foster a culture in which safe, respectful and responsible use of technology is understood and modelled by everyone.

Staff are expected to:

- act as positive role models
- encourage respectful digital behaviour
- challenge unsafe practices where appropriate
- support children in developing confidence, resilience and responsible digital habits
- By promoting positive digital citizenship, the organisation seeks to empower children to engage safely and confidently in an increasingly digital world.

Section 11 – Monitoring, Quality Assurance and Policy Review

11.1 Monitoring Compliance

Bouncing Statistics is committed to ensuring that this policy is implemented consistently and remains effective in promoting a safe digital environment for children, young people and staff.

Compliance with this policy will be monitored through a range of quality assurance activities to ensure that safeguarding arrangements remain robust, proportionate and responsive to emerging risks.

Monitoring activities may include:

- safeguarding supervision and case discussions
- review of CPOMS records and safeguarding trends
- observations of professional practice
- staff feedback and consultation
- review of online safety incidents and lessons learned
- audits of organisational procedures and documentation
- evaluation of training and professional development

review of filtering, monitoring and cyber security arrangements where applicable.

Monitoring findings will be used to identify strengths, areas for development and opportunities to improve practice.

11.2 Quality Assurance

Online safety forms part of the organisation's wider safeguarding quality assurance framework.

The Designated Safeguarding Lead (DSL), together with the Directors, will regularly review:

- the effectiveness of safeguarding responses to online concerns
- staff confidence and compliance with organisational procedures
- emerging trends and patterns of online risk
- the effectiveness of training and awareness activities
- the suitability of technological safeguards
- feedback from children, families, commissioning schools and partner organisations where appropriate

Where improvements are identified, appropriate actions will be incorporated into the organisation's safeguarding improvement planning.

11.3 Continuous Improvement

Bouncing Statistics recognises that technology, digital behaviours and safeguarding risks continue to evolve.

The organisation is committed to continuously improving its online safety arrangements through:

- reviewing safeguarding incidents
- responding to changes in legislation and statutory guidance
- learning from safeguarding practice reviews
- consulting with staff and partner organisations
- responding to emerging technologies and digital risks

reviewing organisational procedures and training

Continuous improvement supports a culture of learning, accountability and safeguarding excellence.

11.4 Policy Review

This policy will be formally reviewed at least annually by the Designated Safeguarding Lead (DSL) and the Directors.

An earlier review will take place where there are:

- significant changes to legislation or statutory guidance
- emerging safeguarding risks
- organisational changes affecting service delivery
- recommendations arising from safeguarding reviews or audits

- changes to organisational technology or digital systems

The most current version of this policy will be made available to all relevant staff and partner organisations.

Section 12 – Related Documents and Policy Statement

12.1 Related Policies

This policy should be read in conjunction with the following organisational policies:

- Safeguarding & Child Protection Policy
- Staff Code of Conduct
- Behaviour Policy
- SEND Policy
- Data Protection Policy
- Confidentiality Policy
- Acceptable Use Policy (where applicable)
- Whistleblowing Policy
- Health & Safety Policy

12.2 Related Standard Operating Procedures (SOPs)

SOP-001 / C-001 – Responding to a Safeguarding Disclosure

SOP-002 / C-002 – Reporting a Safeguarding Concern

SOP-003 / C-003 – CPOMS Recording Standards

SOP-004 / C-004 – DSL Decision-Making & Thresholds

SOP-009 / C-009 – Information Sharing & Confidentiality

SOP-013 / C-013 – Multi-Agency Working & Professional Challenge

SOP-016 / C-016 – Safeguarding Action Tracker

C-015 – Safeguarding Escalation & Emergency Response

C-017 – Online Safety Concern Flowchart

12.3 Related Forms, Registers and Guidance

Supporting documentation may include:

- Individual Risk Assessment
- Safeguarding Action Tracker
- Staff Induction Checklist
- Online Safety Risk Assessment (where required)
- Acceptable Use Agreements
- Visitor Code of Conduct
- Staff Training Records

12.4 Responsibilities for Implementation

Online Safety Risk Assessment (where required)

Staff Acceptable Use Agreement / Digital Conduct Guidance

Online Safety Concern Flowchart C-017

The successful implementation of this policy relies upon the collective responsibility of everyone working within, or on behalf of, Bouncing Statistics.

All staff are expected to:

- understand and comply with this policy
- maintain appropriate professional standards when using technology
- promote safe and responsible digital behaviour
- report concerns promptly
- participate in safeguarding and online safety training
- contribute to a culture of continuous improvement

Managers, the Designated Safeguarding Lead (DSL) and the Directors will support staff in fulfilling these responsibilities through effective leadership, training, supervision and quality assurance.

12.5 Policy Statement

Bouncing Statistics is committed to creating an environment where technology is used safely, responsibly and positively to enhance learning, wellbeing and opportunity.

We recognise that online safety is an integral component of safeguarding and child protection. By embedding robust safeguarding arrangements, promoting positive digital citizenship and responding effectively to emerging risks, we aim to protect children, young people and staff while enabling them to benefit from the opportunities that digital technology provides.

This policy reflects our commitment to continuous improvement, professional accountability and the highest standards of safeguarding practice.

Document Title	Online Safety & Digital Safeguarding Policy
Organisation	Bouncing Statistics CIC
Policy Owner	Designated Safeguarding Lead (DSL)
Approved By	Directors
Responsible Committee	Board of Directors
Version	Version 1.2
Approval Date	August 2026
Effective Date	August 2026
Review Date	(12 months from approval)
Classification	Public / Internal Policy
Related Documents	Safeguarding & Child Protection Policy, Behaviour Policy, Staff Code of Conduct, Data Protection Policy, Acceptable Use Agreement, Whistleblowing Policy, SEND Policy, CPOMS Procedures, Safeguarding SOPs