



storybrook

Online Safety Policy





Contents

1. Purpose and aims
2. Scope
3. Legal and statutory framework
4. Roles and responsibilities
5. Understanding online safety and the four areas of risk
6. Additional vulnerability and Storyybrook's SEMH context
7. Education and the online safety curriculum
8. Safe use of technology and internet access
9. Generative AI and emerging technologies
10. Social media, gaming and online communication
11. Child-on-child online abuse and cyberbullying
12. Sharing nudes and semi-nudes and harmful sexual behaviour
13. Online exploitation, grooming and radicalisation
14. Filtering and monitoring
15. Responding to online safety incidents and safeguarding concerns
16. Staff use of technology and professional boundaries
17. Personal devices and mobile technology
18. Images, video, school website and social media
19. Data protection, privacy and cyber security
20. Working with parents and carers
21. Training
22. Monitoring, governance and review





1. Purpose and aims

Storyybrook recognises online safety as an integral part of safeguarding. Children may experience harm, abuse or exploitation through technology both within and outside school. This policy sets out how the school promotes safe, responsible and positive use of technology while protecting pupils from online harm.

As a specialist SEMH setting, Storyybrook recognises that some pupils may have additional online vulnerabilities linked to factors such as impulsivity, emotional regulation, social communication, a need for belonging or validation, previous trauma and difficulty interpreting the intentions of others. Online concerns will therefore be considered in the context of each pupil's needs and circumstances and responded to in a calm, relational and non-judgemental way.

Storyybrook aims to ensure that pupils are taught to use technology safely and respectfully, staff understand their safeguarding responsibilities, appropriate filtering and monitoring arrangements are in place, concerns are identified and escalated promptly, and emerging risks are considered as technology develops.

This policy should be read alongside Storyybrook's Safeguarding and Child Protection Policy, Filtering and Monitoring Policy, Behaviour and Relationships Policy, Anti-Bullying Policy, Mobile Phone Policy, Staff Code of Conduct, Data Protection Policy and Acceptable Use arrangements.

2. Scope

This policy applies to pupils, staff, agency and temporary staff, trainees, volunteers, governors, contractors, external professionals, visitors and, where relevant, parents and carers.

It applies to school-owned and personal devices, internet and network access, websites, apps, online learning platforms, social media, gaming, messaging, live-streaming, cloud services, cameras and recording technology, artificial intelligence and generative AI, wearable or connected technology and other digital services used in connection with the school.

The policy applies on the school site and during school-organised activities, educational visits, off-site provision and remote learning where applicable. Where online activity outside school affects the safety or welfare of a pupil or has safeguarding implications for the school community, Storyybrook will respond in accordance with its safeguarding responsibilities.

3. Legal and statutory framework

This policy has been developed with regard to current safeguarding, education, data protection and online safety legislation and guidance, including:

- Keeping Children Safe in Education 2026
- Working Together to Safeguard Children 2026
- the Education (Independent School Standards) Regulations 2014
- the Children Acts 1989 and 2004

Date Last Reviewed: 28.08.2026 | Scheduled Review Date: 28.08.2027

Review By: R. Burbridge





- the Education Act 2002
- the Counter-Terrorism and Security Act 2015 and current Prevent duty guidance
- the Equality Act 2010 and Human Rights Act 1998
- the Data Protection Act 2018, UK GDPR and the Data (Use and Access) Act 2025
- Department for Education filtering and monitoring standards and relevant guidance on generative AI and technology safety

Keeping Children Safe in Education identifies online safety as part of safeguarding and groups online risk into four broad areas: content, contact, conduct and commerce. Storybrook applies these principles through safeguarding practice, education, filtering and monitoring, staff training and governance oversight.

4. Roles and responsibilities

Designated Safeguarding Lead

The DSL takes lead responsibility for online safety as part of their wider safeguarding role. The DSL maintains an up-to-date understanding of online risks, ensures concerns are recognised and responded to appropriately, reviews relevant filtering and monitoring information and works with the Headteacher, IT support and external agencies where required. The DDSL supports this work and acts in accordance with safeguarding arrangements when the DSL is unavailable.

Headteacher

The Headteacher has overall operational responsibility for effective implementation of this policy, including ensuring appropriate systems, resources, training, curriculum provision and clearly allocated responsibilities. Where the Headteacher is also the DSL, these responsibilities are exercised together while maintaining clarity between operational leadership and safeguarding decision-making.

IT support and technical providers

IT support or technical providers are responsible for the technical implementation and maintenance of filtering, monitoring and security controls, for reporting significant failures or risks promptly and for providing sufficient information to enable the DSL and Headteacher to understand how systems operate. Technical staff do not make safeguarding decisions on behalf of the DSL.

All staff

All staff are responsible for modelling safe and professional use of technology, supervising pupils appropriately, remaining alert to online harm, following acceptable use arrangements and reporting safeguarding concerns to the DSL or DDSL without delay. Staff must not investigate potential abuse or illegal online activity themselves.

Proprietor and Governing Body

The Proprietor retains strategic responsibility for safeguarding and for ensuring appropriate online safety, filtering and monitoring arrangements are in place. Governance provides

Date Last Reviewed: 28.08.2026 | Scheduled Review Date: 28.08.2027

Review By: R. Burbridge





oversight, challenge and assurance that responsibilities are clear, arrangements are reviewed and identified weaknesses are addressed.

5. Understanding online safety and the four areas of risk

Storyybrook considers online risk through the four broad and interrelated areas identified in statutory guidance:

Content: exposure to illegal, inappropriate or harmful material, including sexual or violent content, self-harm or suicide content, discriminatory or extremist material, misinformation, harmful challenges and AI-generated or manipulated content.

Contact: harmful interaction with other people online, including grooming, coercion, exploitation, radicalisation, deceptive identities and unsafe interactions through social media, messaging, gaming, live-streaming or AI-enabled services.

Conduct: harmful online behaviour by or towards a pupil, including cyberbullying, harassment, sharing nudes or semi-nudes, harmful sexual behaviour, impersonation, non-consensual recording or sharing and harmful use of AI or digital tools.

Commerce: harmful commercial activity, including scams, phishing, fraud, gambling or gambling-like features, in-game purchases, financial exploitation and manipulative advertising or design.

These risks will be considered alongside each pupil's age, development, communication needs, SEND, SEMH needs, lived experience and individual vulnerabilities.

6. Additional vulnerability and Storyybrook's SEMH context

Some pupils with SEND or SEMH needs may find it more difficult to recognise manipulation, coercion, unsafe relationships or the consequences of sharing information. They may also be particularly affected by online rejection, conflict, exclusion or pressure to belong.

Staff will remain professionally curious about changes in behaviour, emotional presentation, sleep, attendance, relationships or device use that may indicate online harm. No single indicator proves abuse. Concerns should be reported rather than investigated by staff.

Responses will be relational and child-centred. A pupil who has taken an online risk may themselves be experiencing abuse, exploitation, coercion or unmet need. Pupils will be supported to seek help without automatic blame or punishment, while appropriate boundaries and accountability remain in place where a pupil has harmed another person.

7. Education and the online safety curriculum

Online safety education is part of Storyybrook's whole-school safeguarding approach and is taught through Relationships and Health Education, PSHE, Computing and wider curriculum and pastoral opportunities.

Teaching will be age and developmentally appropriate and will include safe and respectful use of technology, healthy online relationships, privacy and security, cyberbullying, consent and boundaries, grooming and exploitation, sharing images, scams and financial risk,

Date Last Reviewed: 28.08.2026 | Scheduled Review Date: 28.08.2027

Review By: R. Burbridge





misinformation and source reliability, age restrictions, AI-generated or manipulated content and how to seek help.

Teaching will be adapted where required through explicit instruction, visual supports, modelling, scenarios, repetition, retrieval and individual or small-group work. Storyybrook will avoid fear-based approaches and will focus on developing pupils' confidence, judgement and help-seeking skills.

Resources and external visitors will be appropriately quality assured and must support, rather than replace, the school's own safeguarding and curriculum responsibilities.

8. Safe use of technology and internet access

Pupils will use school technology within clear expectations, appropriate supervision and the school's Acceptable Use arrangements. School-managed devices and networks will be protected by appropriate filtering and monitoring, but technical controls will not replace supervision, education or professional curiosity.

Websites, apps and online services used with pupils will be considered for educational purpose, age suitability, safeguarding, privacy, data protection, accessibility, communication features and other relevant risks. Services will not be used where risks cannot be managed appropriately.

Pupils and staff must not deliberately bypass safeguards, interfere with systems, share passwords, use another person's account or install unauthorised software. Technical failures, inappropriate access and cyber security concerns must be reported promptly.

If a pupil encounters harmful content, staff should respond calmly, avoid unnecessary viewing or sharing and report any safeguarding concern in accordance with section 15.

9. Generative AI and emerging technologies

Storyybrook recognises that generative AI and other emerging technologies may support learning and accessibility but may also create safeguarding, privacy and data protection risks. These include inaccurate or biased information, deepfakes and synthetic media, impersonation, sexualised or abusive manipulated content, scams, grooming, harmful advice and inappropriate interactions with AI chatbots or companion technologies.

Pupils will only use generative AI for school purposes where authorised and appropriately supervised. They will be taught that AI-generated information may be inaccurate or misleading, that generated media may not be genuine and that AI must not be used to bully, humiliate, impersonate, threaten, deceive or harm another person.

Personal, confidential, safeguarding or special category information must not be entered into unapproved AI systems. Before approving an AI-enabled service, Storyybrook will consider its purpose, age restrictions, safeguarding, privacy, data protection, cyber security, accessibility, filtering and monitoring implications and the level of adult oversight required. AI-related incidents will be managed according to the underlying safeguarding concern. New or significantly changed technologies will prompt review of relevant risk assessments, filtering and monitoring, data protection, training and curriculum arrangements where

Date Last Reviewed: 28.08.2026 | Scheduled Review Date: 28.08.2027

Review By: R. Burbridge





appropriate.

10. Social media, gaming and online communication

Storyybrook recognises that social media, gaming and online communication can provide positive opportunities for learning, play, creativity and relationships, while also exposing pupils to privacy, content, contact, bullying, exploitation and commercial risks.

Pupils will be supported to understand age restrictions, privacy, personal information, unknown contacts, screenshots and redistribution, group-chat pressure, live-streaming, in-game communication and purchases, scams, harmful challenges and how to block, report, leave an unsafe interaction and seek adult help.

Concerns about grooming, exploitation, harmful sexual behaviour, radicalisation or child-on-child abuse will be managed under the relevant sections of this policy and the school's safeguarding procedures rather than being treated simply as misuse of a particular platform.

11. Child-on-child online abuse and cyberbullying

Children can abuse, harm or exploit other children online as well as in person. Online abuse may include cyberbullying, harassment, threats, discriminatory or humiliating content, deliberate exclusion, impersonation, non-consensual sharing of images or information, coercion, controlling behaviour, sexual harassment and harmful use of manipulated or AI-generated material.

Online abuse will not be dismissed as banter, joking or part of growing up. A single post, image or message may have an ongoing impact where it is copied or redistributed. Incidents may occur outside school and still require safeguarding action where they affect a pupil's safety or welfare or have implications for the school community.

Staff must report safeguarding concerns to the DSL or DDSL without delay. The school will consider the needs of the child who has experienced harm and, separately, the safeguarding, developmental and support needs of any child who has displayed harmful behaviour. Responses will avoid victim-blaming and will include appropriate protective action, support, boundaries and consequences.

12. Sharing nudes and semi-nudes and harmful sexual behaviour

Sharing nudes and semi-nudes and technology-assisted harmful sexual behaviour are safeguarding matters. This includes the creation, request, capture, sharing or redistribution of nude or semi-nude images, videos or live streams involving children, including sexualised deepfakes or other manipulated content.

Staff who become aware of such an incident must respond calmly, report it immediately to the DSL or DDSL and make a factual safeguarding record. Staff must not ask a child to send or forward imagery, ask another person to obtain it, copy, print, save, screenshot or distribute it, conduct their own investigation or search for additional imagery. Staff should not normally view nude or semi-nude imagery of a child.

The DSL will lead the response and consider the children's age and development, how and why the content was created, consent, coercion, exploitation, threats, power imbalance,

Date Last Reviewed: 28.08.2026 | Scheduled Review Date: 28.08.2027

Review By: R. Burbridge





distribution, adult involvement, wider risk, SEND and SEMH needs and whether external safeguarding or police involvement is required. The DSL should not normally view imagery and will follow current national guidance where there is a compelling safeguarding reason to do so.

The needs of the child who has experienced harm and any child who has created, requested or shared harmful material will be considered separately. Parents and carers will normally be involved unless this would increase risk, compromise an investigation or conflict with safeguarding advice. Explicit imagery must not be attached to safeguarding records or retained by staff.

13. Online exploitation, grooming and radicalisation

Technology may be used to groom, manipulate, coerce or exploit children for sexual, criminal, financial, ideological or other abusive purposes. Grooming may be carried out by adults or children and may initially appear to the child as friendship, affection, belonging, opportunity or support.

Indicators may include secretive or significantly older online contacts, unexplained gifts or digital currency, pressure to communicate privately, requests for personal information or imagery, threats, blackmail, demands for money, pressure to undertake tasks or criminal activity, or changes in behaviour, wellbeing, sleep, attendance or relationships.

Storybrook recognises financially motivated sexual extortion, including threats to share genuine or manipulated sexual material unless a child provides money, further imagery or complies with demands. Children will be supported without blame and should not be encouraged to continue contact or comply with demands in order to gather evidence.

Online radicalisation may occur through social media, messaging, gaming, forums, recommendation systems, misinformation, conspiracy narratives or direct contact. Staff will report concerns to the DSL in accordance with safeguarding and Prevent arrangements and will avoid assumptions based solely on a child's identity, background, beliefs or isolated comments.

Staff must not confront a suspected perpetrator, communicate using the child's account, conduct their own investigation or unnecessarily search, copy or forward harmful material. The DSL will determine the required safeguarding response and any referral to children's social care, police, Prevent or other agencies.

14. Filtering and monitoring

Appropriate filtering and monitoring are essential safeguarding controls. Filtering reduces access to harmful or inappropriate content and monitoring supports identification of concerning activity. No system can eliminate all online risk, and technical controls do not replace supervision, education or safeguarding practice.

The DSL leads on the safeguarding and online safety aspects of filtering and monitoring. IT support or the technical provider is responsible for technical operation and maintenance. The Proprietor retains strategic oversight. Detailed arrangements, including checks,





reporting, review and technical responsibilities, are set out in Storybrook's Filtering and Monitoring Policy.

Filtering and monitoring provision will be formally reviewed at least once every academic year and sooner where significant safeguarding concerns, changes in working practice, new technology, major software changes or technical configuration changes indicate that review is required. The review will include appropriate checks that filtering and monitoring arrangements are operating effectively. The review, checks undertaken, findings and resulting actions will be recorded.

15. Responding to online safety incidents and safeguarding concerns

Online incidents will be responded to according to their nature and safeguarding context rather than solely according to the platform, device or location involved. Where a child may have experienced or be at risk of abuse, neglect, exploitation or other harm, the matter will be managed as a safeguarding concern.

Staff must remain calm, listen carefully, take the concern seriously, avoid blame, report safeguarding concerns to the DSL or DDSL without delay and make a factual record. Staff must not promise confidentiality, undertake their own investigation or unnecessarily search for, view, copy, download, screenshot, forward or share harmful or potentially illegal material.

The DSL will consider immediate safety, the nature and seriousness of the concern, other children who may be at risk, possible abuse, exploitation, coercion or criminality, ongoing circulation of content, the pupil's needs and vulnerabilities, whether parents or carers should be informed and whether external advice or referral is required.

Where an incident indicates a weakness in filtering, monitoring, supervision, staff practice or another safeguarding control, appropriate action will be taken to reduce the risk of recurrence. Information will be shared only on a need-to-know basis, with wider learning anonymised where appropriate.

16. Staff use of technology and professional boundaries

The same professional and safeguarding standards apply online as in face-to-face interactions. Staff must use approved systems for professional communication, maintain appropriate boundaries, protect passwords and confidential information and follow the Staff Code of Conduct and Acceptable Use arrangements.

Staff must not establish personal online relationships with pupils, communicate through personal social media or unauthorised messaging services, exchange personal contact details without legitimate authorisation or permit pupils to use staff accounts. Personal devices must not be used to photograph or record pupils unless specifically authorised under school procedures.

Online conduct by an adult that raises a safeguarding or professional-boundary concern will be considered under the Safeguarding and Child Protection Policy, Staff Code of Conduct, Low-Level Concerns Policy and Managing Allegations Policy as appropriate.

Date Last Reviewed: 28.08.2026 | Scheduled Review Date: 28.08.2027

Review By: R. Burbridge





17. Personal devices and mobile technology

Use of personal devices is governed by Storyybrook's Mobile Phone Policy and Acceptable Use arrangements. Pupils must not use mobile phones or other personal communication devices throughout the school day, including during lessons, transitions, breaktimes and lunchtimes, except where a specific exception has been authorised in accordance with Storyybrook's Mobile Phone Policy.

Where authorised, devices must not be used to photograph or record others without permission, access or distribute harmful material, bully or harass, or bypass school safeguards using hotspots, VPNs, proxy services or similar methods. Staff, visitors and contractors must maintain confidentiality and comply with school expectations for personal devices, photography and recording.

Any search, examination, confiscation or handling of a pupil's device will be undertaken in accordance with applicable law, statutory guidance and school procedures. Safeguarding concerns arising from a personal device will be referred to the DSL or DDSL.

18. Images, video, school website and social media

Images, video and other digital media may be used to celebrate learning and communicate about school life where this is compatible with pupils' privacy, dignity and safety. Images will be created, stored and shared only for legitimate and authorised purposes using approved devices and systems and appropriate consent and privacy arrangements.

Identifying information will not be unnecessarily published alongside images. School websites and social media will be managed by authorised staff with regard to safeguarding, confidentiality, data protection, copyright and the risk that information may reveal a pupil's identity or location.

Staff will remain alert to the possibility that images may be copied, manipulated or used to create deepfakes or other harmful material. Parents, carers and visitors are expected to comply with school arrangements for photography and recording at school events.

19. Data protection, privacy and cyber security

Online safety, data protection and cyber security are closely connected. Personal information will be processed in accordance with applicable data protection legislation and Storyybrook's Data Protection Policy, and access will be restricted according to role and legitimate need.

The school will maintain appropriate account security, system updates, access controls and procedures for reporting data breaches and cyber incidents. Monitoring information will only be accessible to appropriately authorised and trained staff.

Where new technology, monitoring systems or AI-enabled processing are likely to create a high risk to individuals' rights and freedoms, a Data Protection Impact Assessment will be completed where required. Privacy information and relevant third-party provider arrangements will be reviewed appropriately.





Cyber incidents that may affect the safety or welfare of a pupil will be reported to the DSL as well as through technical and data protection procedures.

20. Working with parents and carers

Storybrook will work in partnership with parents and carers to promote safe and responsible use of technology. Information and guidance may include acceptable use, filtering and monitoring, social media and gaming, age restrictions, parental controls, emerging risks, help-seeking and routes for reporting concerns.

Parents and carers will be encouraged to maintain open, non-judgemental conversations about online experiences. Removing access to technology is not always the safest response where fear of losing a device may discourage a child from seeking help.

Parents and carers will normally be informed of significant incidents involving their child unless this could increase risk, compromise an investigation or conflict with safeguarding advice. They are expected to protect the privacy and safeguarding of other children when taking or sharing photographs, videos or information connected with the school.

Legitimate concerns and complaints should be raised through appropriate school channels. Nothing in this policy prevents a parent or carer from raising a concern, making a complaint, reporting a safeguarding matter or exercising another lawful right.

21. Training

Online safety forms part of the school's safeguarding training arrangements and induction. Training will be appropriate to role and will be updated to reflect changes in technology, statutory guidance, safeguarding risks and school practice.

Staff training will include recognition and response to online abuse, grooming and exploitation, child-on-child abuse, sharing nudes and semi-nudes, harmful sexual behaviour, radicalisation, generative AI and manipulated content, professional boundaries, filtering and monitoring, data protection, cyber security and the additional vulnerabilities that may affect pupils with SEND or SEMH needs.

Staff with specific DSL, filtering, monitoring or technical responsibilities will receive additional role-appropriate training. Learning from incidents, reviews and emerging risks will inform future training where appropriate.

22. Monitoring, governance and review

The DSL and Headteacher will keep the effectiveness of online safety arrangements under review using safeguarding concerns and incidents, patterns and trends, pupil voice, filtering and monitoring information, staff concerns, curriculum needs and changes in technology or statutory guidance.

The Proprietor retains strategic responsibility and governance will provide appropriate oversight and challenge. Assurance will include that filtering and monitoring provision is reviewed at least once every academic year, responsibilities remain clear and identified actions are completed. Detailed review and checking arrangements are set out in the Filtering and Monitoring Policy.

Date Last Reviewed: 28.08.2026 | Scheduled Review Date: 28.08.2027

Review By: R. Burbridge





This Online Safety Policy will be reviewed at least annually and sooner where legislation or statutory guidance changes, significant safeguarding learning arises, new technology materially changes the school's risk profile or school systems and practice change. Relevant changes will be communicated to staff and incorporated into training, curriculum and operational practice as appropriate.





Appendix 1: Acceptable use of technology: agreement for parents and carers

Acceptable use of technology: agreement for parents and carers

Name of parent/carers:

Name of child:

Online communication is an important part of school and family life. Storyybrook asks parents and carers to help protect the privacy, dignity and safeguarding of all children.

When communicating about the school, I will:

- communicate respectfully with staff, other parents and children
- raise concerns or complaints through appropriate school channels so that they can be considered and responded to
- protect confidential or sensitive information about pupils and families
- avoid naming or enabling the identification of other children when discussing incidents
- follow school arrangements for photography and recording at school events
- contact the school promptly if I become aware of an online safeguarding concern affecting a child.

I understand that nothing in this agreement prevents me from raising a legitimate concern, making a complaint, reporting a safeguarding matter or exercising another lawful right.

I will not:

- use online communication to bully, harass, threaten or target staff, pupils or other families
- publish confidential information about another child or family
- share photographs or videos of children other than my own unless this is consistent with school arrangements and appropriate permission has been obtained.

Signed:

Date:





Appendix 2: Acceptable use of technology: Storyybrook pupils

Acceptable use of technology: Storyybrook pupils

Name of child:

Date:

At Storyybrook, we want everyone to feel safe, respected, and ready to learn. This agreement helps us work together to use the technology and online services safely and responsibly.

As a pupil, I agree to:

Stay safe online

I will tell a trusted adult straight away if I see or hear anything online that makes me feel worried, upset, or uncomfortable

I will not share personal information (such as my full name, address, phone number, or school) online

Use technology responsibly

I will only use the internet and devices when an adult says it is okay

I will only visit websites or use apps that a teacher has approved

I will follow the school's rules for using devices and online services

Be kind and respectful

I will be polite and respectful to others when using technology

I will not send unkind messages or take part in cyberbullying

I will not share or post anything that could hurt or upset someone else

Take care of school equipment

I will use devices carefully and for learning purposes

I will not try to change settings, download apps, or access blocked content

Ask for help when I need it

I understand that mistakes can happen, and I will ask for help if something goes wrong

I know that adults in school are here to support me and keep me safe





Storyybrook promises:

- to help me learn how to stay safe online
- to listen to me and support me if I have a problem
- to provide safe and supervised internet access

Pupil Signature:

Staff Signature:

Parent/ Carer Signature:

