Brooke Primary Academy

Online Safety Policy

1	Summary	Online Safety Policy			
2	Responsible person	Vikki Watson			
3	Accountable SLT member	Vikki Watson			
4	Applies to	☐All staff ☒Support staff ☒Teaching staff			
5	Who has overseen development of this policy	Vikki Watson			
6	Who has been consulted and recommended policy for approval	SLT			
7	Approved by and date	01/09/2026			
8	Version number	1			
9	Available on	Every	☐Y ☒N	Trust website Academy website SharePoint	☐Y ☐N ☒Y ☐N ☒Y ☐N
10	Related documents (if applicable)				
11	Disseminated to	☐Trustees/governors ☒All staff ☐Support staff ☐Teaching staff			
12	Date of implementation (when shared)	01/09/2026			
13	Consulted with recognised trade unions	☐Y ☒N			

Contents

1. Key Staff 3
2. Links to other policies and national guidance 3
3. Guidance to be read in conjunction with this policy 3
4. Aims and Objectives 4
5. Teaching and Learning 4
6. Staff Training 5
7. Support for Parents/Carers 5
8. Response to an Online Safety Incident of Concern 6
9. Email and Digital Communication 6
10. Social Networking 6
11. Publishing Pupils' Images and Work 7
12. Digital and Video Images 7
13. Online Publishing 7
14. Managing Emerging Technologies, Mobile Phones and Devices 7
15. Managing ICT Systems and Access 8
16. Logins and Passwords 8
17. Managing Filtering and Monitoring 8
18. Data Protection and Online Safety 9
19. Review 9

1. Key Staff

The Principal has overall responsibility for ensuring that online safety arrangements are effective and that online safety forms part of the school's safeguarding culture.

- Principal / Online Safety Lead: Vikki Watson
- Designated Safeguarding Lead (DSL): Vikki Watson
- Deputy DSLs: Lynsey Baxter, Jade Chowings
- SENDCo: Vikki Watson

Responsibilities for online safety are shared across the school. All staff have a responsibility to promote safe and responsible use of technology and to report concerns promptly.

2. Links to other policies and national guidance

- Safeguarding and Child Protection Policy
- Behaviour and Relationships Policy
- Anti-Bullying Policy
- Acceptable Use Agreements
- Data Protection Policy
- Staff Code of Conduct
- Mobile Phone Policy
- Remote Education arrangements, where applicable

3. Guidance to be read in conjunction with this policy

- Keeping Children Safe in Education 2026
- Teaching online safety in schools
- Education for a Connected World Framework

- Department for Education guidance on filtering and monitoring
- Department for Education mobile phone guidance
- Data protection guidance for schools

4. Aims and Objectives

New technologies inspire children to be creative, communicate and learn. However, while the internet is a great resource, it is important that children and young people are protected from the risks they may encounter. Brooke Primary Academy seeks to highlight both the benefits and risks of using technology and to educate and safeguard all users so that they can make safe, responsible and informed choices online.

We believe that the key to developing safe and responsible behaviours online, not only for pupils but everyone within our school community, lies in effective education. The internet and other technologies are embedded in pupils' lives both in school and in the wider world. We therefore have a duty to help pupils safely benefit from the opportunities technology brings.

Online safety risks are considered across four broad areas:

- Content – being exposed to illegal, inappropriate or harmful material, including misinformation, disinformation, extremist or hateful content, pornography, self-harm content and other harmful material.

- Contact – harmful interaction with other users, including peer pressure, bullying, grooming, exploitation, coercion and adults misrepresenting themselves online.

- Conduct – online behaviour that causes or increases the likelihood of harm, including cyberbullying, harassment, sharing inappropriate images and creating or forwarding harmful content.

- Commerce – risks including scams, phishing, inappropriate advertising, financial exploitation, gambling and other harmful commercial activity.

Online safety is a safeguarding responsibility and is considered alongside the school's wider safeguarding, behaviour, anti-bullying and curriculum arrangements.

5. Teaching and Learning

Brooke Primary Academy has a planned approach to online safety which is embedded throughout the curriculum. Online safety is taught through Computing, PSHE/RSHE, assemblies and wider opportunities across the curriculum.

The school will:

- Provide regular opportunities for pupils to discuss, practise and revisit online safety.
- Promote safer internet use through whole-school activities, including Safer Internet Day where appropriate.
- Teach pupils to protect personal information and understand the consequences of sharing information online.
- Teach pupils to consider the accuracy, reliability and purpose of online information, including misinformation and disinformation.
- Teach pupils about respectful online communication and the impact of online bullying and harassment.

- Teach pupils how to seek help if they encounter harmful, upsetting or inappropriate content or behaviour.
- Discuss the safe and age-appropriate use of social media, gaming, apps, streaming services and other online platforms.
- Teach pupils about online reputation, digital footprints, privacy and appropriate use of images.
- Teach pupils that online content may be manipulated or misleading and that AI-generated content, including deepfakes, may not be authentic.

Staff will ensure that internet use is carefully planned, age appropriate and supports the learning objective. Pupils will be taught to use age-appropriate online tools safely and effectively. Staff will model safe and responsible use of technology.

When pupils search the internet, staff will guide them towards age-appropriate search tools and remind them what to do if they encounter unsuitable content. Pupils will be taught that they should stop, close the content where safe to do so and tell a trusted adult.

6. Staff Training

Staff receive regular information and training on online safety, safeguarding and emerging online risks, with updates provided when significant new issues arise.

- As part of induction, staff receive information about this policy, acceptable use, online security, filtering and monitoring and reporting procedures.
- All staff will know how to report online safety concerns and misuse of technology.
- Staff will understand their individual responsibilities for safeguarding children online.
- Staff will be aware that online bullying, harassment, grooming, exploitation and sexual abuse can occur online.
- Staff will understand how online sexual harassment and the sharing of nude or semi-nude images can form part of child-on-child abuse and know how to respond in line with safeguarding procedures.
- Staff will understand the risks associated with AI, manipulated images, deepfakes and misinformation.

7. Support for Parents/Carers

The school will take every opportunity to help parents and carers understand online safety and the risks children may encounter.

- Publish this Online Safety Policy on the school website.
- Provide parents and carers with information and signposting through the school website, newsletters, workshops and other appropriate communications.
- Provide age-appropriate guidance about social media, gaming, apps, devices, parental controls and online wellbeing.
- Signpost parents and carers to organisations including Internet Matters, NSPCC, Childline, CEOP, Childnet and Thinkuknow.
- Use concerns raised through lessons or other school activity as opportunities to provide parents and carers with appropriate advice and support.

Brooke's website provides an online safety section with guidance for parents on social media, parental controls, gaming, inappropriate content, online grooming, online pornography, online reputation, privacy, radicalisation, self-harm and sexting.

8. Response to an Online Safety Incident of Concern

All staff, volunteers and pupils have a responsibility to report online safety incidents so that they can be dealt with effectively and promptly. Concerns may relate to technology used in school or outside school where the concern has an impact on the safety or wellbeing of a pupil or member of the school community.
Online safety concerns should be recorded on CPOMS and reported to the DSL or appropriate member of SLT. Staff should preserve relevant evidence where appropriate and should not investigate safeguarding concerns beyond their role.

- Immediate safeguarding concerns will be dealt with in accordance with the Safeguarding and Child Protection Policy.
- Parents/carers will be informed where appropriate and where doing so does not place a child at further risk.
- Serious concerns may be referred to the police, CEOP or other appropriate agencies.
- Where online bullying is identified, the Anti-Bullying Policy and Behaviour and Relationships Policy will also apply.
- Where a data breach or loss of personal information is suspected, the school's data protection procedures must be followed.

9. Email and Digital Communication

Staff will use school-provided email accounts and approved communication systems for professional purposes. Personal email accounts must not be used for school business or to communicate directly with pupils or parents/carers.

- Staff should not email pupils using personal accounts.
- Professional communication should be appropriate, respectful and consistent with the Staff Code of Conduct.
- Sensitive or personal information must only be shared using approved secure systems.
- Communication with parents/carers should take place through approved school systems such as Arbor or other Trust-approved platforms.

10. Social Networking

The school recognises that social media can provide opportunities for communication and community engagement but also presents risks to privacy, reputation and safeguarding.

Staff should:

- Maintain appropriate privacy settings on personal social media accounts.
- Not accept or initiate personal social media connections with current pupils.
- Not engage in online discussions about confidential or personal matters concerning pupils, parents/carers or colleagues.
- Not post material that could bring the school, Trust or members of the school community into disrepute.
- Act as positive role models in their use of social media.
- Report online harassment, threats or abuse involving the school community through the appropriate school procedures.

The school may respond to publicly available social media content where it raises safeguarding, behaviour, reputational or other legitimate concerns. Parents/carers with concerns about the school are encouraged to contact the school directly rather than attempting to resolve matters through social media.

11. Publishing Pupils' Images and Work

Pupils will only create or publish online content using platforms and systems approved by the school. Staff will model safe and responsible behaviour when creating and publishing online content.

- Pupils' personal information will be protected.
- Full names will not normally be published alongside photographs or videos on public-facing platforms.
- Appropriate consent will be obtained for the use of pupils' photographs, videos or other identifiable material in accordance with the school's data protection arrangements.
- Staff will check relevant permissions before publishing images or work.

12. Digital and Video Images

The school will educate users about the risks associated with digital images and will implement arrangements to reduce the potential for harm.

- Staff and volunteers must know which pupils have restrictions on the taking or publication of images.
- Personal devices must not be used to take photographs or videos of pupils for school purposes.
- School devices and approved systems must be used for school photography and recording.
- Images and recordings must be stored securely and only retained for as long as required.
- Parents/carers attending school events should follow the school's arrangements for photography and should respect the privacy of other children and families.

13. Online Publishing

The school communicates with parents/carers and the wider community through approved online platforms, which may include:

- The school website
- School social media accounts
- Online newsletters
- Arbor and other approved communication platforms

Any online publishing will follow the school's safeguarding, data protection, copyright and communication arrangements. Where pupil work, images or videos are published, pupils' identities and personal information will be appropriately protected.

The school website is managed/hosted by Jon Robson (Digital Schools). The school ensures that online safety policy has been followed in the use of online publishing e.g., use of digital and video images, copyright, identification of young people, publication of school calendars and personal information – ensuring that there is least risk to members of the school community, through such publications.

14. Managing Emerging Technologies, Mobile Phones and Devices

Emerging technologies will be considered for educational benefit and assessed for safeguarding, privacy and other risks before they are introduced into school.

Staff and personal devices

- Personal mobile phones and smart devices must not be used to take photographs or recordings of pupils.

- Personal devices must be used in accordance with the Staff Code of Conduct and acceptable use arrangements.
- Staff should not use personal devices to communicate directly with pupils.

Pupils

- Mobile phones and other smart devices are managed in accordance with the school's Behaviour and Relationships Policy and Mobile Phone Policy.
- Where a pupil is permitted to bring a mobile phone to school, it must be switched off and stored in accordance with school procedures.
- Smart watches and other connected devices must not be used in a way that allows pupils to communicate or access content inappropriately during the school day.
- School devices may be provided for learning activities under appropriate supervision.

The school follows the statutory expectation that pupils should not have access to mobile phones throughout the school day, including lessons, breaktimes and lunchtimes, unless an appropriate exception applies.

15. Managing ICT Systems and Access

The school will determine which users have access to ICT systems and the level of access and supervision required. Access will be appropriate to the user's role, age and need.

- Users must follow the relevant Acceptable Use Agreement.
- Users must take responsibility for their use of school ICT systems.
- School ICT activity may be monitored and checked.
- Access rights will be reviewed when staff or pupils change role or leave the school.
- Devices and systems must be used in accordance with Trust ICT and cyber-security arrangements.

16. Logins and Passwords

Pupils may require usernames and passwords to access approved online learning platforms. These credentials should be kept secure and must not be shared.

- Passwords must not be shared with other pupils or unauthorised users.
- Staff must follow Trust requirements for password security and authentication.
- Where home access is provided, login information should be communicated securely to parents/carers.
- Staff should report suspected compromised accounts promptly.

17. Managing Filtering and Monitoring

The school has a responsibility to provide appropriate filtering and monitoring systems and to review their effectiveness regularly. Technical filtering is supported through the Trust's ICT arrangements.

Filtering is designed to reduce access to illegal, inappropriate and harmful content. Monitoring helps identify potentially harmful or inappropriate activity. No filtering system can remove all risk, so technical systems are supported by active supervision, education and safeguarding procedures.

- The school will review filtering and monitoring provision at least annually and following significant changes to systems or identified risks.
- Filtering and monitoring checks will be recorded.
- Staff will be aware of how to escalate concerns identified through filtering or monitoring.
- Staff must physically supervise pupils when using devices and remain alert to inappropriate use.
- Any unsuitable website, content or system issue identified by staff or pupils must be reported promptly to the Online Safety Lead / ICT support.
- Filtering and monitoring arrangements will be considered in relation to pupils' age, vulnerability and use of technology.

Physical monitoring by staff remains essential. If an issue arises, staff should address it appropriately, provide teaching and support where needed and record safeguarding concerns on CPOMS.

18. Data Protection and Online Safety

Data protection is an important part of online safety because personal information must be protected from unauthorised access, loss or disclosure.

- Personal and sensitive information should only be stored on approved secure systems and devices.
- Staff must take care when sharing personal information and use approved secure communication systems.
- Staff must not store school data on personal devices or personal cloud storage unless expressly authorised by the Trust.
- Any suspected data breach must be reported promptly in accordance with the Trust Data Protection Policy.

19. Review

This policy will be reviewed annually, or sooner where there are significant changes to statutory guidance, technology, school systems or identified online safety risks.