Online Safety Policy

September 2026

	Person responsible/Signature	Date
Approved by:	**Ilona Wyld**	
Last reviewed:	**Mr M Allen**	**Sept 2026**
Next Review Date due:	**Mrs M Fellows / Mr M Allen**	**July 2028**

Contents

1. Aims……3

2. Legislation and guidance……..3

3. Roles and responsibilities……3

4. Educating pupils about online safety……6

5. Policy Summary for children……8

6. Curriculum…..……..8

7. Prevent Duty……...……..9

8. Data Protection……..……...9

9. Use of digital and video images……..……..10

10. Educating parents about online safety……10

11. Cyber bullying……..11

12. Acceptable use of the Internet in school……...……11

13. Staff using work devices outside school……12

14. Pupils using mobile devices in school……..……12

15. Communications ……...12

16. Unsuitable and inappropriate activities……13

17. Training……..14

18. Monitoring Arrangements……15

19. Managed Service Provider……15

20. Technical infrastructure, equipment, filtering & monitoring……..……15

21. Links with other policies……...16

Appendix 1 Staff Acceptable Use Agreement
Appendix 2 EYFS Acceptable Use Agreement
Appendix 3 KS1 Acceptable Use Agreement
Appendix 4 KS2 Acceptable Use Agreement
Appendix 5 Online safety training needs – self audit for staff
Appendix 6 Letter to parents- mobile phone permission
Appendix 7 Employee leavers checklist

1. Aims

Brook Primary school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers, and governors.
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology.
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate.
- Instil our five core values: Respect, Resilience, Pride, Challenge & Independence, in doing so we teach the school community to use online safely and independently, with respect for themselves and others.

The four areas of online safety risk

- In line with Keeping Children Safe in Education 2026, Brook Primary School recognises that online safety risks can be categorised into four areas:
- **Content:** being exposed to illegal, inappropriate or harmful content, including pornography, racism, misogyny, self-harm, suicide, antisemitism, radicalisation, extremism, misinformation, disinformation and conspiracy theories.
- **Contact:** being subjected to harmful online interaction with other users or generative AI applications that simulate interaction, including peer pressure, inappropriate commercial advertising and adults posing as children or young adults to groom or exploit them.
- **Conduct:** online behaviour that increases the likelihood of, or causes, harm, including online bullying and making, sending or receiving explicit images, including images that have been digitally manipulated or generated using AI.
- **Commerce:** risks including online gambling, inappropriate advertising, phishing and financial scams.

2. Legislation and guidance

This policy is based on the Department for Education's (DfE) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- Relationships and sex education
- Searching, screening and confiscation

It also refers to the DfE's guidance on protecting children from radicalisation.

Relationships Education

This policy is linked with the DFE Relationships and Sex Education (RSE) and Health Education statutory guidance, effective from 1 September 2026.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

The policy also takes into account the National Curriculum computing programmes of study which state:

Key stage One:
Pupils should be taught to use technology safely and respectfully, keeping personal information private; identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies.

Key stage Two:
Pupils should be taught to use technology safely, respectfully and responsibly; recognise acceptable/unacceptable behaviour; identify a range of ways to report concerns about content and contact.

3. Roles and responsibilities

3.1 The governing board

The governing board has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.

The governing board will make sure all staff undergo online safety training as part of child protection and safeguarding training, and ensure staff understand their expectations, roles and responsibilities around filtering and monitoring.

The governing board will co-ordinate regular meetings with appropriate staff to discuss online safety and monitor online safety logs as provided by the designated safeguarding lead (DSL).

The governing board should ensure children are taught how to keep themselves and others safe, including keeping safe online.
The governing board must ensure the school has appropriate filtering and monitoring systems in place on school devices and school networks, and will regularly review their effectiveness. The board will review the DfE's filtering and monitoring standards, and discuss with IT staff and service providers what needs to be done to support the school in meeting the standards, which include:

- Identifying and assigning roles and responsibilities to manage filtering and monitoring systems;
- Reviewing filtering and monitoring provisions at least annually;
- Blocking harmful and inappropriate content without unreasonably impacting teaching and learning;
- Having effective monitoring strategies in place that meet their safeguarding needs.

The governor who oversees online safety is Kath Poole (Safeguarding Governor)

All governors will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's IT systems and the internet (appendix 1)
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with special educational needs and/or disabilities (SEND). This is because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable

3.2 The headteacher

The headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

3.3 The designated safeguarding lead

At Brook Primary the DSL is Miss Sheryl Nicklin alongside the DSL deputies: Mrs Marie Fellows, Mr Matthew Allen, Miss Hannah Didlock, Mrs Rebecca Taylor and Mrs Stacey Waterworth.

The DSL takes lead responsibility for online safety in school, in particular:

- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school.
- Working with the headteacher, Computing lead and other staff, as necessary, to address any online safety issues or incidents.
- Taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and school network
- Providing governors with assurance that filtering and monitoring systems are working effectively and reviewed regularly
- Working with the ICT manager to make sure the appropriate systems and processes are in place
- Working with the headteacher, ICT manager and other staff, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the school's child protection policy
- Responding to safeguarding concerns identified by filtering and monitoring
- Ensuring that any online safety incidents are monitored and dealt with appropriately in line with this policy.
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy.
- Updating and delivering staff training on online safety (appendix 5 contains a self-audit for staff on online safety training needs).
- Liaising with other agencies and/or external services if necessary.
- Providing regular reports on online safety in school to the headteacher and/or governing board.
- Undertaking annual risk assessments that consider and reflect the risks children face
- Providing regular safeguarding and child protection updates, including online safety, to all staff, at least annually, in order to continue to provide them with relevant skills and knowledge to safeguard effectively

This list is not intended to be exhaustive.

3.4 The Computing Lead

The Computing Lead is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems on school devices and school networks, which are reviewed and updated at least annually to assess effectiveness and ensure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material - Classroom Cloud
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly.
- Conducting a full security check and monitoring the school's ICT systems monthly supported by Network IT24.
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files.
- Ensuring that any online safety incidents are monitored and dealt with appropriately in line with this policy.
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy.

This list is not intended to be exhaustive.

3.5 All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (appendix 1), and ensuring that pupils follow the school's terms on acceptable use.
- Knowing that the DSL is responsible for the filtering and monitoring systems and processes, and being aware of how to report any incidents of those systems or processes failing by reporting them to the DSL
- Following the correct procedures by reporting to the DSL if they need to bypass the filtering and monitoring systems for educational purposes
- Working with the DSL and business manager to ensure that any online safety incidents are addressed and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline, and maintaining an attitude of 'it could happen here'
- All staff receive regular Online Safety training and reminders so that they understand their responsibilities, as outlined in this policy. Training is offered as follows:
- A planned programme of formal online-safety training is made available to staff. It is anticipated that some staff may identify online safety as a training need within the performance management process.
- All new staff receive an Online Safety briefing as part of their induction programme, ensuring that they fully understand the school Online Safety Policy and Acceptable Use Policies.
- The H&S/Online Safety lead, DSL and Computing lead receive updates through attendance at Local Authority training sessions. They review guidance documents released by DfE and LA and others.
- This Online Safety policy and its updates are presented to and discussed by staff in staff/ meetings/INSET days and briefings.

This list is not intended to be exhaustive.

3.6 Parents

Parents are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy.

Parents can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues? - UK Safer Internet Centre
- Online safety topics for parents/carers - Childnet
- Parent factsheet - Childnet

3.7 School Business manager

The school business manager will ensure that the employee leaving checklist (appendix 7) has been carried out and that all devices have been returned. The school business manager, alongside the computing lead, will ensure that access to all school systems is withdrawn on the date an employee leaves the school.

3.8 Visitors and members of the community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (appendix 1).

4. Educating pupils about online safety

Pupils will be taught about online safety as part of the curriculum:

All Primary schools have to teach: Relationships education and health education.

In **Key Stage 1**, pupils will be taught to:

- Use technology safely and respectfully, keeping personal information private.
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies.

Pupils in **Key Stage 2** will be taught to:

- Use technology safely, respectfully and responsibly
- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and contact
- Be discerning in evaluating digital content

By the **end of primary school**, pupils will know:

- That people sometimes behave differently online, including by pretending to be someone they are not.
- That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online including when we are anonymous.
- The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them.
- How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met.
- How information and data is shared and used online.
- What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context)
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know
- The benefits of rationing time spent online, the risks of excessive time spent on electronic devices and the impact of positive and negative content online on their own and others' mental and physical wellbeing
- How to consider the effect of their online actions on others and know how to recognise and display respectful behaviour online and the importance of keeping personal information private
- Where and how to report concerns and get support with issues online

The safe use of social media and the internet will also be covered in other subjects where relevant.

Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND.

4.1 E-Safety and the Curriculum

There is a planned and progressive E-Safety/E-literacy curriculum. Learning opportunities are embedded into the curriculum throughout the school and are taught in all year groups.

E-Safety education is provided in the following ways:

- A planned E-Safety programme is provided as part of computing/PHSE /other lessons and is regularly revisited – this includes the use of ICT and new technologies in school and outside school.
- Key E-Safety messages are reinforced as part of a planned programme of assemblies.
- Pupils are taught in all lessons to be critically aware of the materials/content they access on-line and be guided to validate the accuracy of information
- Pupils are aware of the Pupil Acceptable Use Policy, reading and signing to indicate they have done so during a computing session, and are encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school.
- Pupils are taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- Rules for use of ICT systems/internet are posted in classrooms and/or are displayed on log-on screens.
- Pupils are taught the importance of information security and the need to keep information such as their password safe and secure.
- Staff act as good role models in their use of ICT, the internet and mobile devices.

Pupils have access to the school network and technologies that enable them to communicate with others beyond the school environment. The network is a secure and safe system provided through IT Network 24.

Pupils:

- Are responsible for using the school ICT systems in accordance with the Pupil Acceptable Use Policy *(see appendix 2,3 and 4*), which they have to read before being given access to school systems.
- Need to have a growing understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- Will be expected to know and understand school policies on the use of mobile phones, digital cameras and hand-held devices. They should also know and understand school policies on the taking/use of images, use of social networking sites and on cyber-bullying.
- Should understand the importance of adopting good E-Safety practice when using digital technologies out of school and realise that the school's E-Safety policy covers their actions out of school, if related to the use of an externally available web-based system or material provided by the school or accessed through school.

5. Policy summary for children

Children should:

- Only use internet sites suitable for their age.
- Only watch films, videos and play music and games that are appropriate for their age. Take notice of the certificate given or warning notice.
- Report any unsuitable material that they may accidentally access or see anyone else accessing.
- Not copy work from the internet, especially large amounts that may be a part of copyright laws.
- Not take pictures of others without their permission and that of their parents or load pictures on to any websites or sharing sites.
- Not normally bring mobile phones into school including for evening events. If they are brought in, hand them in immediately to a teacher with parental permission. (Year 5 & 6 only)

- Understand that online services, social-media platforms, games and apps may have minimum-age requirements and that pupils should use technology in accordance with age restrictions, parental guidance and the school's online-safety education.
- Not communicate with strangers on the internet in any way.
- Never agree to meet with anyone they have only met online. Tell their parents or any adult they trust if anyone asks this.
- Only use mobile phones, email or messaging services for respectful communications. Remember cyber-bullying is as serious as other sorts of bullying.
- Keep passwords secret, not share them and change them regularly.

6. Curriculum

E-Safety is a focus in all areas of the curriculum and staff re-enforce E-Safety messages in the use of ICT across the curriculum.

- In lessons, where internet use is pre-planned, students/pupils are guided to sites checked as suitable for their use and there are processes in place for dealing with any unsuitable material that is found in internet searches - ICE, a search engine can be used to ensure pupil's access to the web is safe.
- Where pupils are allowed to freely search the internet, e.g. using search engines, staff should monitor the content of the websites the young people visit.
- The school provides opportunities within a range of curriculum areas to teach about E-Safety
- It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Network Manager or managed service provider temporarily remove those sites from the filtered list for the period of study. Any requests to do so are auditable and should be logged.
- Pupils are taught in all lessons to be critically aware of the materials/content they access on-line and are guided to validate the accuracy of information.
- Pupils are taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet. Pupils are aware of the impact of Cyber-bullying and know how to seek help if they are affected by any form of online bullying. Pupils are also aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent/ carer, teacher/trusted staff member, or an organisation such as Childline.
- Printing should be for display of work or inclusion in books/portfolios only and should be with the permission of the class teacher.

7. The Prevent Duty

The statutory guidance makes clear the need for schools to ensure that children are safe from terrorist and extremist material when accessing the internet in schools. Schools should ensure that suitable filtering is in place.

The school recognises that it has an important role to play in equipping children to stay safe online, both in school and outside. Internet safety is integral to a school's ICT curriculum and can also be embedded in PSHE and RSE.
As with other online risks of harm, every teacher needs to be aware of the risks posed by the online activity of extremist and terrorist groups.

The school's filtering and monitoring arrangements will be informed by and reviewed in the context of the school's Prevent Duty risk assessment.

8. Data Protection

The school will comply with current data protection legislation, including the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 and the Data (Use and Access) Act 2025, together referred to as data protection laws.

Personal information will be processed lawfully, fairly and transparently and will be appropriately protected against unauthorised or unlawful processing, accidental loss, destruction or damage.

Everyone responsible for using personal data has to follow strict rules called 'data protection principles' unless an exemption applies.

Personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection.

Staff are aware of the Dudley Information Security Policy.

Staff ensure that they:

- Take care at all times, to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Access personal data on secure password protected computers and other devices ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.
- Will only transfer personal data using school-approved secure systems and in accordance with the school's Data Protection and Information Security policies.
- Personal data should not normally be stored on any portable computer system, USB stick or any other removable media. Permission to store and remove personal data should be sought from the Head or Deputy. Any such data must be encrypted and password protected and be deleted once work has been completed and saved securely in school.

9. Use of digital and video images

- When using digital images, staff inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. They recognise the risks attached to publishing their own images on the internet e.g. on social networking sites, though primary pupils are advised not to use Facebook and similar sites.
- Staff are allowed to take digital/video images to support educational aims, and follow school policies concerning the sharing, distribution and publication of those images. Those images are only taken on school equipment, the personal equipment of staff are not used for such purposes e.g. cameras on mobile phones.
- Pupils are not permitted to use personal digital equipment, including mobile phones and cameras, to record images of the others, this includes when on field trips.

- Care is taken when capturing digital/video images, ensuring pupils are appropriately dressed and that they are not participating in activities that might bring the individuals or the school into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission and that of their parents.
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and comply with good practice guidance on the use of such images.
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Written permission from parents or carers is obtained before photographs of students /pupils are published on the school website.
- Pupil's work can only be published with the permission of the pupil and parents or carers. Parents should have signed the DSCB consent form.

10. Educating parents about online safety

The school will raise parents' awareness of internet safety in letters or other communications home, and in information via our website or Google Classrooms. This policy will also be shared with parents.

Online safety will also be covered during parents' evenings.

The school will let parents/carers know what systems the school uses to filter and monitor online use

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the headteacher and/or the DSL.

Concerns or queries about this policy can be raised with any member of staff or the headteacher.

11. Cyber-bullying

11.1 Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy.)

11.2 Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Class teachers will discuss cyber-bullying with their year groups.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training (see section 11 for more detail).

The school also sends information/leaflets on cyber-bullying to parents so that they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will consider whether the incident should be reported to the police if it involves illegal material and will work with external services if it is deemed necessary to do so.

11.3 Artificial Intelligence (AI)

Generative artificial intelligence (AI) tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Gemini.

Generative AI risks include:

- inappropriate AI-generated content;
- interaction with AI/chatbot services;
- misinformation and fabricated content;
- AI-generated or manipulated images;
- deepfakes;
- bullying using AI;
- safeguarding risks associated with pupil-facing AI;
- personal/confidential information being submitted to AI systems;
- age restrictions associated with services;
- data protection;
- intellectual property;
- inappropriate reliance on AI-generated information.

Brook Primary School recognises that AI has many uses to help pupils learn, but may also have the potential to be used to bully others. For example, in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real.

Brook Primary School will treat any use of AI to bully pupils very seriously, in line with our Anti-bullying/Behaviour policy.

Staff should be aware of the risks of using AI tools whilst they are still being developed and should carry out a risk assessment where new AI tools are being used by the school, and where existing AI tools are used in cases which may pose a risk to all individuals that may be affected by it, including, but not limited to, pupils and staff.

Staff must not enter identifiable pupil information, safeguarding information, special category data or confidential school information into generative AI systems unless the system has been formally approved by the school and its use complies with the school's data protection arrangements.

12. Acceptable use of the internet in school

All pupils, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school’s ICT systems and the internet (appendices 1-4). Visitors will be expected to read and agree to the school’s terms on acceptable use if relevant.

Use of the school’s internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual’s role.

We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.

More information is set out in the acceptable use agreements in appendices 1-4.

13. Staff using work devices outside school

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- Keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol)
- Ensuring their hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device
- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends
- Installing anti-virus and anti-spyware software
- Keeping operating systems up to date – always install the latest updates

Staff members must not use the device in any way which would violate the school's terms of acceptable use, as set out in appendix 1.

If staff have any concerns over the security of their device, they must seek advice from the Headteacher.

13.1. Remote working

This policy works in conjunction with the school's remote learning policy. The key points are listed below:

- Staff should ensure that when teaching online lessons, the children's cameras should be turned off
- All online lessons should be delivered through the class Google classroom
- Staff should be appropriately dressed when teaching live lessons
- Staff should uphold professional standards at all times
- Use a blurred or neutral background image when on video

14. Pupils using mobile devices in school

Brook Primary School is a mobile-phone-free environment throughout the school day. Pupils must not have access to mobile phones or other smart communication technology, such as SMART watches during the school day.

Pupils in year 5 & 6 only, may bring mobile devices into school, but are not permitted to use them during:

- Lessons
- Clubs before or after school, or any other activities organised by the school

Exceptions may be made where required as a reasonable adjustment for disability or SEND, to support a medical condition, or where there are other exceptional individual circumstances. Such arrangements will be agreed by the Headteacher/DSL and documented appropriately.

Any use of mobile devices in school by pupils must be in line with the acceptable use agreement and parental permission must be given. (Appendix 6)

Any breach of the acceptable use agreement by a pupil may trigger disciplinary action in line with the school behaviour policy, which may result in the confiscation of their device.

15. Communications

When using communication technologies the school considers the following as good practice:

- The official school email service may be regarded as safe and secure and is monitored. Staff and pupils should therefore use only the school email service to communicate with others when in school, or on school systems e.g. by remote access from home- *(If staff use none standard or personal email accounts these are not secure and should not be used for school business).*
- Users need to be aware that email communications may be monitored.
- Users must immediately report, to the nominated person (Head or Deputy) – in accordance with the school policy, the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.
- Any digital communication between staff and students/pupils or parents/carers must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or public chat/social networking programmes must not be used for these communications.
- Pupils are provided with individual school email addresses for educational use.
- Pupils should be taught about email safety issues, such as the risks attached to the use of personal details. They should also be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material.
- Personal information should not be posted on the school website and only the info address should be stated not individual emails.
- The school allows staff to bring in personal mobile phones and devices for their own use. Under no circumstances should a member of staff contact a pupil or parent/ carer using their personal device unless authorised to do so by the school. Mobiles should not normally be kept on the person during lessons and never whilst changing a child or helping with toileting. Mobile phones can however be taken on school visits for contacting school and/or in emergencies.
- The school is not responsible for the loss, damage or theft of any personal mobile device.
- The sending of inappropriate text messages between any member of the school community is not allowed.
- Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device.
- The school provides a safe and secure way of using chat rooms, blogs and other 'social networking technologies'. Other social networking options should not be used in school. School offers guidelines for staff on the related use of social networking off site/out of normal working hours.

16. Unsuitable/inappropriate activities

All monitoring, surveillance or investigative activities are conducted by ICT authorised staff and comply with the Data Protection Act 2018, the Human Rights Act 1998, the Regulation of Investigatory Powers Act 2000 (RIPA) and the Lawful Business Practice Regulations 2000.

The school will take all reasonable precautions to ensure E-Safety.

However, owing to the international scale and linked nature of internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a school computer or mobile device.

Staff and pupils are given information about infringements in use and possible sanctions. Sanctions available include:

- Interview/counselling by Class Teacher/H and S/E-Safety Coordinator/Head teacher.
- Informing parents or carers.
- Removal of internet or computer access for a period, (which could ultimately prevent access to files held on the system).
- Referral to LA/Police.

Our H & S/E-Safety Coordinator acts as first point of contact for any complaint. Any complaint about staff misuse is referred to the Headteacher.

- Complaints of cyber-bullying are dealt with in accordance with our Anti-Bullying Policy.
- Complaints related to child protection are dealt with in accordance with school/LA child protection procedures.

There are however a range of activities which may, generally, be legal but would be inappropriate in a school context, either because of the age of the users or the nature of those activities.

Nude and semi-nude images, including AI-generated imagery

Any incident involving the making, sharing or possession of nude or semi-nude imagery involving a child, including imagery that has been digitally manipulated or wholly generated using artificial intelligence, will be treated as a safeguarding concern and reported immediately to the DSL or a deputy.

Staff will follow the school's Child Protection and Safeguarding Policy and relevant national guidance. Staff must not intentionally view, copy, print, save or share such imagery unless specifically required as part of an authorised safeguarding or law-enforcement process.

16.1 How the school will respond to issues of misuse

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in our policies on behaviour and ICT and internet acceptable use. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary procedures/staff code of conduct. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

17. Training

Online safety training will be integrated and aligned with the school's whole-school safeguarding approach, wider staff training and curriculum planning.

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required.

By way of this training, all staff will be made aware that:

- Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse
- Children can abuse their peers online through:
  - Abusive, threatening, harassing and misogynistic messages
  - Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
  - Sharing of abusive images and pornography, to those who don't want to receive such content
- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element

Training will also help staff:

- Develop better awareness to assist in spotting the signs and symptoms of online abuse
- Develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh up the risks
- Develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term

The DSL and deputies will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our child protection and safeguarding policy.

17.1 Pupils

All pupils will receive age-appropriate training on safe internet use, including:

- Methods that hackers use to trick people into disclosing personal information
- Password security
- Social engineering
- The risks of removable storage devices (e.g. USBs)
- Multi-factor authentication
- How to report a cyber incident or attack
- How to report a personal data breach

Pupils will also receive age-appropriate training on safeguarding issues such as cyberbullying and the risks of online radicalisation.

18. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety using the CPoms system.

This policy will be reviewed at least annually and sooner where there are significant changes to statutory guidance, technology, emerging online risks or the school's filtering and monitoring provision.

19. Managed service provider

The managed service provider is responsible for helping the school to ensure that it meets the E-Safety technical requirements outlined by NetworkIT24. The managed service provides a number of tools to schools including,

Classroom Cloud, Surf Protect and Quantum Filtering, which are designed to help schools keep users safe when on-line in school.

NetworkIT24 work with school representatives to develop and update any E-Safety policy and guidance.

Members of the NetworkIT24 will support schools to improve their E-Safety strategy.

The managed service provider maintains backups of email traffic for 90 days. If access to this information is required, the school can contact the NetworkIT24.

NetworkIT24 ensure the Headteacher is made aware of any inappropriate use of technology via 'Classroom Cloud' global software. The Headteacher and business manager are notified via email of any inappropriate use via search engines is used by staff or pupils. Any misuse will be recorded on the school's CPOM system and addressed by the DSL or SLT.

20. Technical – infrastructure/equipment, filtering and monitoring

The managed service provider is responsible for ensuring that the school infrastructure/ network is as safe and secure as is reasonably possible. The school is responsible for ensuring that policies and procedures approved within this policy are implemented.

School ICT systems will be managed in ways that ensure that the school meets the E-Safety technical requirements outlined in the Acceptable Use Policies

Senior Leader Responsible for Filtering and Monitoring
The Headteacher will delegate Mrs Vicky Baker (Business manager) as the senior leader responsible for filtering and monitoring. As part of governor visits, the use of Classroom cloud is monitored and discussed.
The named senior leader will lead a review of the effectiveness of the school's filtering and monitoring provision **at least once every academic year**, supported by the DSL and the school's IT support provider.

The review will include checks that filtering and monitoring operate appropriately on **all internet-connected school devices and in all relevant locations**.

A written record of these checks, identified concerns and resulting actions will be maintained.
The review will consider the ages and needs of pupils, including pupils who may be at greater risk of harm, emerging online threats and developments in generative AI.

- There will be regular review of the safety and security of school ICT systems.
- Servers, wireless systems and cabling must be securely located and physical access restricted.

All users will have clearly defined access rights to school ICT systems:

- All users will be provided with a username and password.
- Staff are encouraged to change their password on a regular basis
- School have class log-ons and passwords for FS (Foundation Stage) pupils, but we are aware of the risks associated with not being able to identify any individual who may have infringed the rules set out in the policy
- Users will be made responsible for the security of their username and password. They must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.
- The school maintains and supports the managed filtering service provided by NetworkIT24.
- The school can provide enhanced user-level filtering through the use of the Classroom Cloud Quantum Filtering.

- The school manages and updates filtering issues through the NetworkIT24 helpdesk.
- Requests from staff for sites to be removed from the filtered list will be considered by the Network Manager and Headteacher.
- The managed service provider ensures that appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, hand held devices etc from accidental or malicious attempts which might threaten the security of the school systems and data.
- An agreed procedure is in place for the provision of temporary access to “guests” (e.g. trainee teachers, visitors) onto limited areas of the school system.
- Files containing pupil’s personal data beyond a name and a limited number of results should not be downloaded to portable media (memory sticks, CD’s/DVD’s).
- The school infrastructure and individual workstations are protected by up to date virus software in line with NetworkIT24 services.
- Workstations and Chrome Books have Classroom Cloud software – alerts sent to the Headteacher if there are any misappropriate searches made by any staff member and pupils and the Head Teacher and School Business Manager will be sent alerts if a pupil attempts to search for anything deemed inappropriate.
- Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.
- Copyright material must only be used as specified by copyright laws.

21. Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure
- ICT and internet acceptable use policy
- Remote Learning Policy

Appendix 1: Staff Acceptable Use Agreement

Acceptable Use Agreement 2026-27 - Staff

Background and purpose

With access to rich dynamic content, connectivity across the globe, a platform for creativity and a place to engage in debate, digital technologies provide a powerful tool for learning. Digital technologies give staff opportunities to enhance children's learning in their care and enable staff to become more efficient in their work. The very nature of digital technologies means that they should be used with care and particular attention given to demonstrating appropriate behaviours and avoidance of misuse at all times.

Professional integrity and strong moral purpose must be upheld at all times by staff. It is the duty of all staff members to ensure that children in their care get the very best start to the world of digital technology. This should include provision of a rich, robust online safety education for the children with clear reporting procedures for infringements to safeguarding. Having a transparent approach to using digital technology is a must. Additionally, staff should develop critical thinking in their children, along with strategies for avoiding unnecessary harm and strategies for dealing with online safety infringements.

The school's internet, network and ICT systems and subscriptions to services should be used with the utmost professionalism at all times. The school will aim to provide its staff with secure systems which will have filtering, monitoring and virus protection included. Anyone with access to the systems should be aware that their use of the systems is monitored, and this can be used to form evidence should any suspected infringements occur.

Acceptable Use Agreement

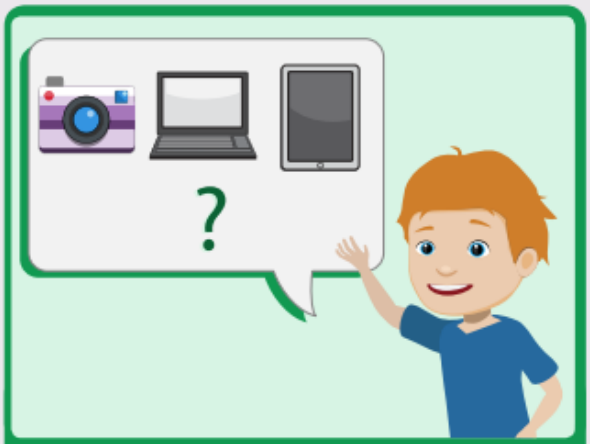
By signing this agreement, you will have access to the school's systems and acknowledge that you agree to all the statements below. Additionally, that you have read and understand school policies which have a bearing on this agreement.

• I will demonstrate the value of the use of digital technologies in improving the outcomes for children in my care. • I will educate children in my care in the safe use of digital technologies, acting on any online safety issues in accordance with the school's policies. • I understand my use of the school's ICT systems/networks and internet are monitored. • I recognise that whether within school or out of school, I must abide by the rules/statements set out in this document when using systems, accessing/transferring data that relate to the school or impact on my role within the school and wider community. • I know what GDPR is and how this has a bearing on how I access, share, store and create data. • Any data that I have access to away from school premises must be kept secure and used with specific purpose. As outlined in the school's data protection policy, it is my responsibility to ensure when accessing data remotely that I take every bit of reasonable care to ensure the integrity and security of the data is maintained. • I understand that I am fully responsible for my behaviours both in and out of school and as such recognise that my digital communications, subscriptions and content I access can have a bearing on my professional role. • I recognise that my social media activity can have a damaging impact on the school and children in my care at school if I fail to uphold my professional integrity at all times whilst using it. • If I am contributing to the school's social media account(s) or website(s) I will follow all guidelines given to me, with particular care given to what images/video imagery and details can be uploaded. • I will never upload images/video imagery of staff/pupils or other stakeholders to my personal social media accounts unless there is	I will inform the school at the earliest opportunity of any infringement both on and off site by myself. Furthermore, if I am concerned about others' behaviours/conduct, I will notify the school at the earliest opportunity. • I will never deliberately access, upload or download illegal, inflammatory, obscene or inappropriate content that may cause harm or upset to others. • I will never download or install software unless permission has been given by the appropriate contact at school. • I shall keep all usernames and passwords safe and never share them. Writing down usernames and passwords, including storing them electronically, constitutes a breach to our data protection and safeguarding policy. • I will never leave equipment unattended which could leave data and information vulnerable; this extends to accessing data/ services/content remotely. • Any personal devices I own shall not be used to access school systems/data/services/content remotely unless I have adequate virus protection and permission from the school. • I understand that mobile devices, shall not be used, nor in my possession (unless on school trips), during times of contact with children. These devices will be securely locked away with adequate password protection on them should they be accessed by an unauthorised person. • Any school trips/outings or activities that require a camera will be given an IPAD to use by the school and any data collected on them will be used in accordance with school policies. • At no point- will I use my own devices for capturing images/ video or making contact with parents/carers (unless on a school trip when number will be withheld)

significant reason to and that permission has been granted by the head teacher in writing for each occurrence.	

Appendix 2: EYFS Acceptable Use Agreement

EYFS ACCEPTABLE USE AGREEMENT



I ask before I use a tablet, computer or camera.

I tap or click on things I have been shown.

I check if I can tap/click on things I haven't seen before.

I tell a grown-up if something upsets me.

My Name:

Class:

Parent/Carer Signed:

Today's Date:

Appendix 3: KS1 Acceptable Use Agreement

KS1 ACCEPTABLE USE AGREEMENT

- ✓ I always ask a teacher or suitable adult if I want to use the computers, tablets or cameras.
- ✓ I only open activities that an adult has told or allowed me to use.
- ✓ I know that I must tell an adult if I see something on a screen that upsets me, or I am unsure of.
- ✓ I keep my passwords safe and will never use someone else's.
- ✓ I know personal information such as my address and birthday should never be shared online.
- ✓ I know I must never communicate with strangers online.
- ✓ I am always polite when I post to our blogs, use our email and other communication tools.

I understand this agreement and know the consequences if I don't follow it.

My Name:	Class:

Parent/Carer Signed:	Today's Date:

Appendix 4: KS2 Acceptable Use Agreement

KS2 ACCEPTABLE USE AGREEMENT

- ✓ I will only access computing equipment when a trusted adult has given me permission and is present.
- ✓ I will not deliberately look for, save or send anything that could make others upset.
- ✓ I will immediately inform an adult if I see something that worries me, or I know is inappropriate.
- ✓ I will keep my username and password secure; this includes not sharing it with others.
- ✓ I understand what personal information is and will never share my own or others' personal information such as phone numbers, home addresses and names.
- ✓ I will always use my own username and password to access the school network and subscription services such as Purple Mash.
- ✓ In order to help keep me and others safe, I know that the school checks my files and the online sites I visit. They will contact my parents/carers if an adult at school is concerned about me.
- ✓ I will respect computing equipment and will immediately notify an adult if I notice something isn't working correctly or is damaged.
- ✓ I will use all communication tools such as email and blogs carefully. I will notify an adult immediately if I notice that someone who isn't approved by the teacher is messaging.
- ✓ Before I share, post or reply to anything online, I will T.H.I.N.K.

  T = is it true?
  H = is it helpful?
  I = is it inspiring?
  N = is it necessary?
  K = is it kind?
- ✓ I understand that if I behave negatively whilst using technology towards other members of the school, my parents/carers will be informed and appropriate actions taken.

I understand this agreement and know the consequences if I don't follow it.

My Name:

Class:

Parent/Carer Signed:

Today's Date:

Appendix 5: online safety training needs – self audit for staff

ONLINE SAFETY TRAINING NEEDS AUDIT	
Name of staff member/volunteer:	**Date**:
Question	**Yes/No (add comments if necessary)**
Do you know the name of the person who has lead responsibility for online safety in school?	
Do you know what you must do if a pupil approaches you with a concern or issue?	
Are you familiar with the school's acceptable use agreement for staff, volunteers, governors and visitors?	
Are you familiar with the school's acceptable use agreement for pupils and parents?	
Do you regularly change your password for accessing the school's ICT systems?	
Are you familiar with the school's approach to tackling cyber-bullying?	
Are there any areas of online safety in which you would like training/further training?	

Appendix 6: Letter to parents- mobile phone permission

Dear Parents & Families,

As a school we recognise that mobile phones are now an important part of everyday life, and both children and adults use them regularly for a range of purposes. However, it is essential that when children bring phones to school, they adhere to the school guidance.

Only children in Year 5 and 6 **who are walking to or from school on their own,** may bring their mobile to school. However, they MUST adhere to the strict guidance OR they will lose this privilege either for a set period of time or permanently as decided by the Headteacher.

1. The phone must be handed in as soon as they enter the classroom, and they will collect it at the end of the day.
2. Phones must **NOT BE USED AT ALL** whilst on school premises.
3. The phone **MUST** be off at all times.
4. The school will take no responsibility whatsoever for lost, stolen, or damaged phones.

If a phone is seen or heard by a member of staff, they will confiscate it and will only return it to a parent/guardian.

If it becomes evident that a child is using or has used a mobile phone on school premises – either as a means of communication OR as a camera – they will no longer be allowed to bring their phone into school.

Any child, in any other year group, must not have a phone in school.

If you would like your child to bring their mobile phone into school, please complete the FORMS by following this link as soon as possible:

Only children with a completed FORMS providing permission will be allowed to bring their phone.

Yours Faithfully,

Mrs M Fellows

Headteacher

Online form example:

Child's Name: _____
Class:_____

I give permission for my child to bring their mobile phone to school but only on days when they are walking to or from school on their own.

I have discussed the rules with my child and understand that the school will take no responsibility whatsoever for lost, stolen or damaged phones.

I understand that the phone may be confiscated if the strict guidance is not adhered to.

Signed:_____ Date:_____

Print Name:_____

Appendix 7: Employee leavers checklist

Brook Primary School - Staff exit checklist

Exiting staff member's name:

Job title:

Leaving date:

TASK	DATE COMPLETED
Respond in writing to the resignation, and formally agree a notice period/last working day	
Inform school staff	
Inform pupils and parents/carers	
Resolve any outstanding expenses or salary claims	
Request the deletion of all school data from personal devices	
Make sure all necessary jobs and information has been handed over	
Request the return of all school equipment	
Provide an exit survey and hold an exit interview	
Remove login access to school IT systems and platforms	
Remove the departing staff member's details from the school's single central record (SCR)	
Update your school website	

This checklist has been completed by:

Job title:

Signature:

Date: