



**Park Brow
Primary School**



Happy - Respect - Pride - Caring - Potential

Online Safety and acceptable use Policy

September 26-27

Approved by:

Governing Body

Date: October 2026

Last reviewed on:

September 2026

Next review due by:

September 2027

Park Brow Primary School aims to have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors.

Delivering an effective approach to online safety, which empowers and educates the whole school community in its use of technology.

Park Brow Primary School has clear mechanisms to identify, intervene and escalate an incident where appropriate

Legislation and guidance

This policy is based on the latest statutory safeguarding guidance, including:

- Keeping Children Safe in Education (KCSIE).
- Working Together to Safeguard Children.
- Teaching Online Safety in Schools.
- Searching, Screening and Confiscation.
- Prevent Duty Guidance.
- Relationships Education, Relationships and Sex Education and Health Education.
- Online Safety Act 2023.
- DfE Filtering and Monitoring Standards.

The school recognises that safeguarding incidents and behaviours can be associated with factors both inside and outside school, including online environments. The school will take a safeguarding-centred approach to online safety and digital technology use.

The policy also takes into account the National Curriculum computing programmes of study.

This policy also takes account of the safeguarding aspects within our PSHE/Jigsaw Scheme of Work.

Filtering and Monitoring The school maintains appropriate filtering and monitoring systems to safeguard pupils and staff when using school technology and internet services.

The Governing Body, Headteacher, Designated Safeguarding Lead (DSL) and IT Lead will ensure that:

- Appropriate filtering and monitoring systems are in place.
- Systems are reviewed regularly to ensure effectiveness.
- Filtering and monitoring arrangements reflect local safeguarding risks.
- Alerts and concerns are reviewed promptly.
- Safeguarding concerns are escalated in accordance with safeguarding procedures.
- Governors receive regular reports regarding online safety, filtering and monitoring arrangements.

The school will not rely solely on filtering and monitoring systems and recognises that effective safeguarding also requires education, supervision, staff vigilance and robust reporting procedures.

Artificial Intelligence (AI)

The school recognises that artificial intelligence technologies are increasingly used by children and adults.

Pupils will be taught how to:

- Critically evaluate AI-generated information.
- Recognise inaccurate, misleading or manipulated content.
- Use technology responsibly and ethically.
- Report concerns regarding harmful or inappropriate AI-generated content.

Staff must ensure that:

- AI is used safely, lawfully and appropriately.
- Confidential or personal information is not uploaded into unauthorised AI systems.
- AI-generated content is checked for accuracy before use.
- Pupils' use of AI remains appropriately supervised.

AI must not be used to create harmful, offensive, discriminatory or misleading content.

Online Risks

Online Risks

The school's curriculum, safeguarding arrangements and behaviour expectations will address the four categories of online risk:

Content

Exposure to illegal, harmful or inappropriate material including:

- Extremism and radicalisation.
- Hate content.
- Online pornography.
- Misinformation and disinformation.
- Harmful online challenges.

Contact

Risks from online interactions including:

- Online grooming.
- Child sexual exploitation.
- Criminal exploitation.
- Coercion.
- Scams and fraud.

Conduct

Risks arising from online behaviour including:

- Cyberbullying.
- Online harassment.
- Child-on-child abuse.
- Sharing inappropriate content.
- Online aggression and discrimination.

Commerce

Risks associated with digital transactions including:

- Gambling.
- Scams.
- Fraudulent purchasing.
- Exploitative advertising.

The school will also respond appropriately to concerns involving livestreaming, social media misuse, online sexual harassment and nude image sharing.

Online Sexual Abuse

Concerns related to:

- Nude image sharing.
- Online sexual harassment.
- Online coercion.
- Sexual exploitation.
- Child-on-child abuse involving technology.

will be managed through the Child Protection and Safeguarding Policy.

All concerns must be reported immediately to the DSL and managed in accordance with statutory safeguarding procedures.

Roles and Responsibilities

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 co-ordinate regular meetings with appropriate staff to discuss online safety, and monitor online safety logs as provided by the designated safeguarding lead (DSL). These will be discussed within Inclusion Governors where a full safeguarding review is provided termly.

The governors who oversee online safety is the Inclusion Governor Committee.

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 ICT systems and the internet.

The Headteacher

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

Details of the school's DSL are set out in our child protection and safeguarding policy as well relevant job descriptions.

The DSL is supported by our IT lead who takes responsibility 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, ICT manager and other staff, as necessary, to address any online safety issues or incidents
- Ensuring that any online safety incidents are logged 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 using CPOMS
- Updating and delivering staff training on online safety
- Providing regular reports on online safety in school to the head teacher and/or governing board
- Ensuring our school website provides advice and support for Parents.

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 and ensuring that pupils follow the school's terms on acceptable use (appendices 3)
- Working with the DSL to ensure that any online safety incidents are logged (see appendix 4) 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.

Parents

Parents are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (appendices 3)

- Signed a user agreement when loaning devices from the school.

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

- What are the issues? - [UK Safer Internet Centre](#)
- Hot topics - [Childnet International](#)
- Parent factsheet - [Childnet International](#)

Park Brow also has a designed online safety section on the school website to support Parents and their children.

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 policy.

Educating pupils about Online Safety

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

From September 2020 **all** schools will have to teach:

Relationships education and health education in primary schools. See PSHE/Jigsaw website for more detailed information.

This new requirement includes aspects about online safety.

As such we've added these expectations **in italics** below,

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

- Use technology safely and respectfully, keeping personal information private

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

Park Brow also has an E-Safety Charter that is known to all pupils (appendix 2)

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*
- *How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know*

The safe use of social media and the internet will also be covered in other subjects where relevant including through our PSHE scheme Jigsaw.

The school will use assemblies to raise pupils' awareness of the dangers that can be encountered online and may also invite speakers to talk to pupils about this.

The school also participates in Safer Internet Week.

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. This will be more frequent during National Lockdowns.

This policy will also be shared with parents.

- Online safety will also be covered during parents' evenings.
- 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

Cyber-bullying 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.)

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 classes, and the issue will be addressed in assemblies.
- 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.

Examining electronic devices

School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or
- Break any of the school rules

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:

- Delete that material, or
- Retain it as evidence (of a criminal offence or a breach of school discipline), and/or ☐ Report it to the police

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

Acceptable use of the internet in school- See appendix 3

Pupils using mobile devices in school-

- Y6 pupils are allowed to bring in mobile phones to school and they are handed into the Class teacher and collected at the end of the day. They must not be used on the school site and parents must fill in a disclaimer. The school will not be held responsible for lost mobile phones.
- Any use of mobile devices in school by pupils must be in line with the acceptable use agreement (see appendix 3).
- 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.

Pupils using mobile devices outside school-

- Under the Dfe device scheme. Pupils may be allocated devices to support online learning during school closure or local lockdown.
- Parents must complete and sign a user agreement for the safe use of IT at home (see appendix 1)
- All devices are secured by the Dfe including systems to report issues online.

Staff using work devices outside school

- Staff members using a work device outside school must not install any unauthorised software on the device and must not use the device in any way which would violate the school's terms of acceptable use.
- Staff must ensure that their work device is secure, encrypted, and password-protected, and that they do not share their password with others. They must take all reasonable steps to ensure the security of their work device when using it outside school. Any USB devices containing data relating to the school must be encrypted.
- If staff have any concerns over the security of their device, they must seek advice from the ICT manager.
- Work devices must be used solely for work activities.

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 Behaviour Policy. 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 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.

Training

- 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 (for example through emails, ebulletins and staff meetings).
- The DSL will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. The IT lead will attend online safety training.
- 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.

Remote Learning (see Remote Learning Policy)

Park Brow's main online platforms include:

Evidence Me, Loom, SEESAW, Oxford Reader, Time Tables Rockstars, Spelling Shed, BBC Bitesize and Oak academy. All of which, where relevant, are GDPR compliant.

Other examples are found on the school website.

- Park Brow uses a variety of online websites to support learning both in school and at home. These are certified DfE recommended resources.
- Live/recorded or voice over power points enable important interaction between teachers and pupils through, for example, questioning, eliciting and reflective discussion.
- Teaching is likely to be more effective, support pupil motivation and lead to better progress.
- Platforms can also be used beyond the individual lesson context for other events such as whole staff briefings and professional development sessions, and for teachers to lead events such as year or whole school assemblies.
- Using the features of a multi-functional platform, teachers can create regular, pre and post lesson quizzes.
- Consideration should be given to ensuring availability for pupils without ready online access, including through distribution of hard-copy versions.
- Monitor a sample of disadvantaged pupils, pupils with EAL and pupils with SEND, since these groups might have extra barriers to remote learning

7. Monitoring and Review (REPLACE EXISTING SECTION)

Monitoring and Review

The Headteacher, DSL and IT Lead will review online safety, filtering and monitoring arrangements throughout the year.

The Governing Body will:

- Receive regular online safety reports.
- Review filtering and monitoring effectiveness annually.
- Monitor emerging risks and safeguarding trends.
- Ensure statutory online safety duties are fulfilled.

This policy will be reviewed annually or sooner if legislation, safeguarding guidance or local circumstances require.

Links with other policies

This online safety policy is linked to our:

- *Child protection and safeguarding policy*
- *Behaviour policy*

- *Data protection policy and privacy notices*
- *Complaints procedure*
- *ICT and internet acceptable use policy*
- *Staff Code of Conduct*
- *Remote Learning Policy.*
- *PSHE/Jigsaw Policy.*



**Park Brow
Primary School**



Happy - Respect - Pride - Caring - Potential

Device loan agreement for pupils

1. This agreement is between:

1) Park Brow Primary School, Southdene, Kirkby, L32 6QH

2) Name of Parent.....

and governs the use and care of devices assigned to the parent's child

Name of child.....

This agreement covers the period from the date the device is issued through to the return date of the device to the school.

All issued equipment shall remain the sole property of the school and is governed by the school's policies.

1. The school is lending the pupil the equipment for the purpose of remote learning.
2. This agreement sets the conditions for taking the school device home.

I confirm that I have read the terms and conditions set out in the agreement and my signature at the end of this agreement confirms that I and the pupil will adhere to the terms of loan.

2. Damage/loss

By signing this agreement I agree to take full responsibility for the loan equipment issued to the pupil and I have read or heard this agreement read aloud and understand the conditions of the agreement.

I understand that I and the pupil are responsible for the equipment at all times whether on the school's property or not.

If the equipment is damaged, lost or stolen, I will immediately inform Ms V Roberts, and I acknowledge that I am responsible for the reasonable costs requested by the

school to repair or replace the equipment. If the equipment is stolen, I will also immediately inform the police.

I agree to keep the equipment in good condition and to return it to the school on their demand from the school in the same condition.

I will not leave the equipment unsupervised in unsecured areas.

I will make sure my child takes the following measures to protect the device:

Keep the device in a secure place when not in use

Don't leave the device in a car or on show at home

Don't eat or drink around the device

Don't lend the device to siblings or friends

Don't leave the equipment unsupervised in unsecured areas

3. Unacceptable use

I am aware that the school monitors the pupil's activity on this device.

I agree that my child will not carry out any activity that constitutes 'unacceptable use'.

This includes, but is not limited to the following:

Using ICT or the internet to bully or harass someone else, or to promote unlawful discrimination

Any illegal conduct, or statements which are deemed to be advocating illegal activity

Activity which defames or disparages the school, or risks bringing the school into disrepute

Causing intentional damage to ICT facilities or materials

Using inappropriate or offensive language

I accept that the school will sanction the pupil, in line with our behaviour policy, if the pupil engages in any of the above **at any time**.

4. Personal use

I agree that the pupil will only use this device for educational purposes and not for personal use and will not loan the equipment to any other person.

5. Data protection

I agree to take the following measures to keep the data on the device protected.

Keep the equipment 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)

Make sure my child locks the equipment if it's left inactive for a period of time

Do not share the equipment among family or friends

Update antivirus and anti-spyware software as required

Install the latest updates to operating systems, as prompted

If I need help doing any of the above, I will contact Mrs O Neil on the email

parkbrow@knowsley.gov.uk

6. Return date

I will return the device in its original condition to within 4 days of being requested to do so.

I will ensure the return of the equipment to the school if the pupil no longer attends the school.

7. Consent

By signing this form, I confirm that I have read and agree to the terms and conditions set out above.

Please sign by typing or signing your name and your child's name.

PUPIL'S FULL NAME

PARENT'S FULL NAME

PARENT'S SIGNATURE

Park Brow's E-Safety Charter

- I will only use the Internet when an adult has said it is safe to do so.
- I will tell an adult if I see anything on the computer that upsets me.
- I will tell an adult if I see anything on the computer that I shouldn't look at.
- I will not give any information about myself on the internet including my name, age address or school.
- I will use IT equipment responsibly and in the way my teacher has asked and taught me to.
- I will treat and respect IT equipment.

ZIP IT: Don't give out personal information.

BLOCK IT: Don't use internet sources that you are unsure about, download things without permission or open messages from unreliable sources.

FLAG IT: Talk to a trusted adult if you see anything that worries you.

APPENDIX 3 ACCEPTABLE USE POLICY



**Park Brow
Primary School**

Happy - Respect - Pride - Caring - Potential



Park Brow Primary School - IT Acceptable Use Policy

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

This Acceptable Use Policy is intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.

The school will try to ensure that pupils will have good access to ICT to enhance their learning and will, in return, expect the students to agree to be responsible users.

Pupils

Please read the content with your child and discuss at an **age appropriate** level. This should be signed by your child as an Internet contract to keep safe online.



You are responsible for good behaviour with the resources and on the Internet just as you are in a classroom or a school corridor. Remember that using the Internet inappropriately will result in you being stopped from using IT in school.

Equipment

- I understand that the school IT systems are there to help me with my learning and they must not be used for anything else unless I have my teacher's permission. ☑ I will tell an adult if any equipment is damaged or not working.
- I will only use my mobile phone or tablet in school if I have permission.
- I will never eat or drink by ICT equipment.

Security and Privacy

- I will always keep my password to myself and never use someone else's logon name or password.
- I will always get permission before showing anyone my home address, telephone number, school name or picture on the Internet.
- I must not be unkind to other computer users.
- I will respect the security on the computers and not attempt to change the settings.
- I understand that my teachers may look at my files and what I have accessed to ensure that I am using the system responsibly.

Internet

- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not use the school ICT systems for on-line gaming, on-line gambling, internet shopping, file sharing or video broadcasting (for example YouTube), unless I have permission from a member of staff.
- I will not try to upload, download or access any materials which are illegal or not appropriate for my age.
- I will not open any emails, unless I know and trust the person/sender.
- I will only use chat and social networking sites with permission and at the times that are allowed.
- I know that people on the Internet are not always who they seem. I must never meet someone I have met on the Internet.

Email

- I will be polite. I will not be unkind and say hurtful things.
- I will only open attachments to emails if they come from someone I know and trust.
- If someone is unkind to me on an email or through social media I will tell an adult.

I have read the school Internet Rules and I will always try to follow them.

Full name:	
Signature:	
Date:	



**Park Brow
Primary School**

Happy - Respect - Pride - Caring - Potential



IT Acceptable Use Policy Agreement - Staff and Other Stakeholders

The school has provided computers for use by staff. The computers are provided and maintained for the benefit of all staff and you are encouraged to use and enjoy these resources and help to ensure they remain available to all. Remember that access is a privilege, not a right and inappropriate use will result in that privilege being withdrawn.

Equipment

- I will not connect any device (including USB drives) to the network that does not have up-to-date anti-virus software.
- USB drives must also be encrypted devices.
- I will not use personal digital cameras or camera phones or digital devices for taking, editing and transferring images or videos of students or staff and will not store any such images or videos at home.
- I will follow the school's policy on use of mobile phones / own devices at school.
- I agree and accept that any computer or laptop loaned to me by the school is provided solely to support my professional responsibilities and that I will notify the school of any "significant personal use."
- I agree that my use of ICT and information systems will always be compatible with my professional role, whether using school or personal systems. This includes the use of email, text, social media, social networking, gaming, web publications and any other devices or websites.
- I understand that any hardware and software provided for staff use can only be used by members of staff and only for educational use. To prevent unauthorised access to systems or personal data, I will not leave any information system unattended without first logging out or locking my login as appropriate.
- I will always get permission before installing, attempting to install or storing programs of any type.
- I will only use the computers for educational purposes. Activities such as buying or selling goods are inappropriate and not acceptable.
- I will always check files brought in on removable media (such as CDs, flash drives etc.) with antivirus software and only use them if they are found to be clean of viruses.
- Always check mobile equipment (e.g. laptops, tablet PCs etc.) with antivirus software and ensure they have been found to be clean of viruses before connecting them to the network.
- I will never eat or drink by ICT equipment.

Security and Privacy

- I will ensure all documents, data etc., are printed, saved, accessed and deleted/shredded in accordance with the school's Information Security Policy.
- I will not allow unauthorised individuals to access e-mail / Internet / intranet / network or other school systems.
- I will ensure any confidential data that I wish to transport from one location to another is protected by encryption and that I follow school data security protocols when using any such data at any location.
- I will not store any personal information on the school computer system that is unrelated to school activities, such as personal photographs, files or financial information. I will respect copyright and intellectual property rights.
- I will keep my password to myself and never use someone else's logon name or password. I will always be wary about revealing my home address, telephone number, school name or picture on the Internet.

- I know that other computer users should be respected and should not be harassed, harmed, offended or insulted.
- I will respect the security on the computers and not attempt to bypass or alter the settings.
- I understand that the Head Teacher may review my files and communications to ensure that I am using the system responsibly.

Internet

- I will access the Internet for school activities only.
- I have read and understood the school Online policy which covers the requirements for safe ICT use, including using appropriate devices, safe use of social media websites and the supervision of students within the classroom and other working spaces.
- I will not attempt to bypass any filtering and/or security systems put in place by the school. If I suspect a computer or system has been damaged or affected by a virus or other malware or if I have lost any school related documents or files, then I will report this as soon as possible.
- I understand that all Internet usage and network usage can be logged, and that this information can be made available to the Head Teacher on their request.
- I will not engage in any online activity that may compromise my professional responsibilities.
- I will not browse, download or send material that could be considered offensive to colleagues.
- I will report any accidental access to, or receipt of inappropriate materials, or any filtering breach or equipment failure to the Head Teacher.
- I will not download any software or resources from the Internet that can compromise the network or is not adequately licensed, or which might allow me to bypass filtering and security systems.
- I will ensure that any private social networking sites / blogs, etc. that I create or actively contribute to are not confused with my school or professional role.
- I will ensure, where used, that I know how to use any social networking sites / tools securely, so as not to compromise my school or professional role.
- I will not create, transmit, display, publish or forward any material that is likely to harass, cause offence, inconvenience or needless anxiety to any other person, or anything which could bring my professional role, the school, or the Council, into disrepute.
- I will only access suitable material; using the Internet to obtain, download, send, print, display or otherwise transmit or gain access to materials which are unlawful, obscene or abusive is not permitted.

Email

- I will only use the school's approved systems to communicate with students and will only do so for teaching and learning purposes i.e. through seesaw or for reasons to facilitate professional communication during a lockdown.
- I will be polite and appreciate that other users might have different views from my own. The use of strong language, swearing or aggressive behaviour is not allowed.
- I will only open attachments to emails if they come from someone I know and trust. Attachments can contain viruses or other programs that could destroy all the files and software on your computer.

- If I receive an email containing material of a violent, dangerous, racist or inappropriate content, I will always report this to the Head Teacher.

Please read this document carefully. Only once it has been signed and returned will access to the Internet be permitted. If you do not here adhere to this policy access to the internet may be denied and you may be subject to disciplinary action. Additional action may be taken by the school in line with existing policy regarding staff behaviour. Where appropriate, police may be involved or other legal action taken.

I have read the Acceptable Use Policy and understand my responsibility to comply with requirements set down within it.	
Full name:	
Relationship to School:	
Signature:	
Date:	



Appendix 3

Social Media Acceptable Use Policy

Staff And Other School Stakeholders

Context:

Social media and other online communication tools are important and powerful but the nature of the internet means that social networking sites can leave teachers and the school they work for vulnerable and open to criticism if they fail to observe some simple precautions. Every comment we make informs opinions about us as people and professionals. The public have a right to expect that we model appropriate behaviour at all times. Our school welcomes the benefits of social media and manages the potential risks through awareness raising, policies and procedures. This acceptable use policy (which has been written to support appropriate, safe and positive use of social technologies) underpins the requirements set out in the safety policy and supports staff members of our school community in ensuring that responsible digital citizenship is a reality.

Using Social Media with Pupils and Within the Context of Learning:

Where adults wish to use social media as part of the teaching and learning process this must have clear education objectives and intended outcomes. Senior leadership/line managers must be kept informed of the planned activities. This supports transparency and helps the school to manage concerns and in some cases objections raised by parents. Key considerations are:

- Children must be old enough to use the social media site. The age restrictions vary, but most stipulate that the user must be 13.
- The privacy options are appropriate and applied.
- Comments are moderated prior to publishing and learners are aware that any content must reflect themselves and their school in a positive light.
- The service used is generally recognised as trusted and reliable.
- Parents/carers have been notified that social learning will be used in their child's teaching.
- Responsive reporting systems are in place.

- The educational value of the activity has been shared with colleagues, learners and parents/carers.
- There is a pastoral/disciplinary process in place in the event of an incident.

Staff should be aware of the supporting processes in place to ensure appropriate actions are taken quickly when incidents happen. This includes how the school can support staff if they are the target of malicious activity online.

A key benefit of social media for schools is the opportunity to communicate directly with parents and carers, and this immediacy can help ensure they have the right information at the right time. Where parents and carers are invited to comment on children's online work, guidance should be provided to ensure all comments are positive and supportive. Despite this, negative comments may be posted and learners should be provided with strategies to cope with this eventuality.

Personal Use of Social Media by Adults Who Work With Children and Young People:

Remember - nothing is private and nothing can be deleted. Whether you're an active user of Facebook or an occasional contributor to online discussions your comments, observations, images, videos, reflections lead people to form an opinion about you and can get you and the school into difficulties. You need to consider carefully what your online profile says about you.

When using social media, staff:

- ✓ Should make it clear that their comments are personal and not representative of the school.
- ✓ Should stay clear of rumours or topics that can be associated with 'public anger'.
- ✓ Should be careful not to compliment or criticise products and services - this could be construed as a professional endorsement.
- ✓ Should consider adding a disclaimer to their social media sites to the effect that any views expressed are those of the individual and not their employer. Putting a disclaimer on a social media site does not excuse content or exonerate the site owner from responsibility and in some cases disciplinary action may result.
- ✓ A disclaimer is not an excuse to post any content you wish to make and does not exonerate you of responsibility.
- ✓ Should ensure that their online conduct complies with the staff code of conduct and must act in accordance with the relevant school policies including the ICT Policy, Online policy and this guidance.
- ✓ Must use the schools approved communication methods. In the case of Twitter – the school has a Twitter account where interactions are controlled, monitored and in accordance with the Online policy.
- ✓ Must be aware of their online profile. Friends and family members may post content that could be misconstrued or considered inappropriate. In these cases, the person who posted the content should be asked to remove it.

When using social media, staff:

- × Should not add parents, carers or children as friends or personal contacts in any social media.
- × Should not engage in any role/school related discussion online (outside of formal channels).
- × Should not make derogatory remarks about their employer/colleagues/pupils or their families.
- × Should not publish their age, home address or other information they would not want their pupils to know.
- × Should not post content that could be considered defamatory, derogatory or in breach of copyright legislation.
- × Must not share personal or confidential information about the school, its staff or pupils online. Examples of this kind of information are staff changes, terms of employment, procurement, business partnerships and personal information about colleagues and children. Information of this kind must never be shared on social media. Where there is a legitimate reason to share information the school business processes must be followed.

Parents and Carers:

Parents sometimes raise concerns about the progress of their child, behaviour concerns etc. via a Facebook wall or message board. In all cases, the appropriate communication processes publicised by the schools should be used. These processes have been designed to support professional and confidential discussion and problem resolution.

Where parents and carers are invited to comment on children's online work, guidance should be provided to ensure all comments are positive and supportive. It is not acceptable for anyone to post negative comments about any child on social media and the school need to be careful to ensure they are not complicit in this occurring.

Final Note:

All school stakeholders are expected to model appropriate online behaviour and good judgement in content published online. The school may be monitoring social media and will take seriously any content that could have a negative implication for the school, its staff, the pupils or the community it serves.

I have read the school social media policy and understand my responsibility to comply with requirements set down within it.	
Full name:	
Relationship to School:	
Signature	
Date:	

--	--



**Park Brow
Primary School**



Happy - Respect - Pride - Caring - Potential

Acceptable Use Policy

Social Media – Pupils

Context:

Social media and other online communication tools can be very useful tools for educational, recreational and personal use if used properly. If not used properly they can cause upset and harm to you and to others. Every comment we put online gives the people who read it an opinion of what we are like as people and we should always try to make sure that we give the best impression because this matters now and in the future. We should also respect other people and not do anything online that could upset them or cause them harm. The law says that your school has a responsibility to help you to stay safe even when you are not in school.

We do not want to stop you being creative online but we do want to help you understand that actions (even those online) have consequences. We expect you to be a good ambassador for your school at all times, including when you are online. This policy and the school ICT Acceptable Use Policy are designed to help you to be a good digital citizen but you are responsible for your behaviour.

Using Social Media in School:

- You must read, understand and sign the school's ICT Acceptable Use Policy. If you do not understand it you must ask a teacher for help.
- You must not use chat or social media sites in school unless you have permission and are allowed to do so.
- You must always follow the instructions given to you. If you are not sure, you must ask your teacher for advice.

Using Social Media Outside School:

Always

- ✓ Check you are old enough to use the social media site. Most sites say that you must be at least 13. This is to protect your personal information and to stop you seeing something that could upset you or may be hurtful or harmful. You should not enter incorrect or false information to join social media networks.
- ✓ Make sure the privacy options are appropriate and applied. If in doubt, ask someone who understands to help you get it right. Remember to check the privacy options often.
- ✓ Use passwords that are hard for other people to guess (use a mix of letters and numbers). Never share or reveal your passwords and change them regularly.
- ✓ Make sure you have anti-virus software installed and keep it up to date.
- ✓ Check a website is secure before you put private information on it – a padlock symbol or https should appear in front or after the web address in the browser.

- ✓ Always think carefully before opening an attachment or clicking on a link or attachment sent from someone you don't know – it could contain a virus.
- ✓ Always unplug your webcam, cover the lens or point it at a blank wall when it's not in use.
- ✓ Always think carefully about what you share online. Things like profile pictures can give strangers clues to where you live.
- ✓ Remember – actions have consequences. You should only post things that you are happy for other people to see. Make sure you send messages only to the people you want to see them.
- ✓ Think carefully before you post especially before posting pictures or videos – these may give strangers clues to where you live.
- ✓ Think carefully before forwarding something you receive or before altering or forwarding pictures posted by someone else.
- ✓ Remember – once you post it you can't get it back. Even if you delete the information from a site you have little control over where it may have already gone.
- ✓ Think before your post. It is important to keep some things about yourself, your family and your friends to yourself. Some information is private and should stay that way but nothing is private online.
- ✓ Be courteous online just as you would be in person and think carefully about the language you use on line. Politeness counts!
- ✓ Create a safe screen name – a good screen name won't reveal much about how old you are, your gender or where you live.
- ✓ Always be careful who you chat to online. Not everyone who contacts you is who they say they are and you should be very careful if you are contacted by someone you don't know. If someone you don't know adds you as a friend, ignore them and delete the request. Check and update your friends list regularly.
- ✓ Remember, not everything you read online is true! Information online may be written from a particular point of view or may be written to mislead you.
- ✓ Be careful when someone tries to get you to spend money online – don't be tempted and keep your information secret.
- ✓ Think carefully about talking about a problem online. Some websites are there to help you but you need to be careful. If in doubt, talk with an adult you can trust.
- ✓ Trust your instinct – if something doesn't feel right it probably isn't.
- ✓ Always tell a trusted adult if you feel uncomfortable or threatened by something that happens online.

- ✓ Remember that once an image is sent or posted, there is no getting it back. Once you send or post a picture online you lose control of who sees it and what happens to it.

Online bullying can make you feel embarrassed, scared or upset. It can seem like it will never end but there are things that you can do to make it stop. If anything makes you feel upset, scared or uncomfortable – tell a trusted adult such as a parent, teacher or someone else you trust.

Never:

- ✗ Never enter incorrect or false information to join social media networks. Age restrictions are in place to protect you from seeing things that may upset you or are there to protect you from risk of harm.
- ✗ Never upload anything that you wouldn't want your parents, teachers or friends to see. Once you send it – it is no longer private.
- ✗ Never create sites, pages or posts that seem to come from someone else. It is wrong to impersonate other people.
- ✗ Never post anything cruel, nasty or offensive even if you are angry about something. You don't know how it will affect someone and you can't take it back. Never spread rumours or post hurtful comments about other people including other pupils and staff at your school. This may be cyberbullying and there could be serious implications for you and the other people involved.
- ✗ Never share personal information like your address or phone number with someone you don't know.
- ✗ Never meet up with people you have met on line – not everyone is who they say they are.
- ✗ Never feel that you are on your own. If there is a problem there are people who can help you. Talk to an adult you can trust.
- ✗ Never take or send explicit pictures of yourself, even if you are in a relationship with the person you are sending them to. Once you have sent an image you lost control of who see it and where it goes.

Final Note:

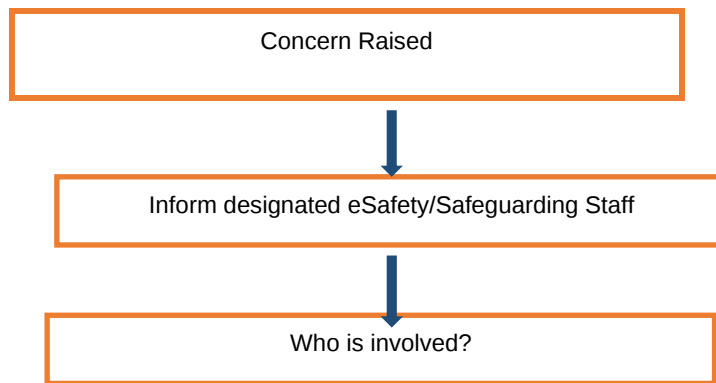
We are proud of our school and all our pupils. Remember we may be monitoring social media and will take seriously any content that could have a negative implication for the school, its staff, its pupils or the community it serves. **DON'T FORGET IF SOMETHING SEEMS LIKE ITS NOT RIGHT THEN REPORT IT!**

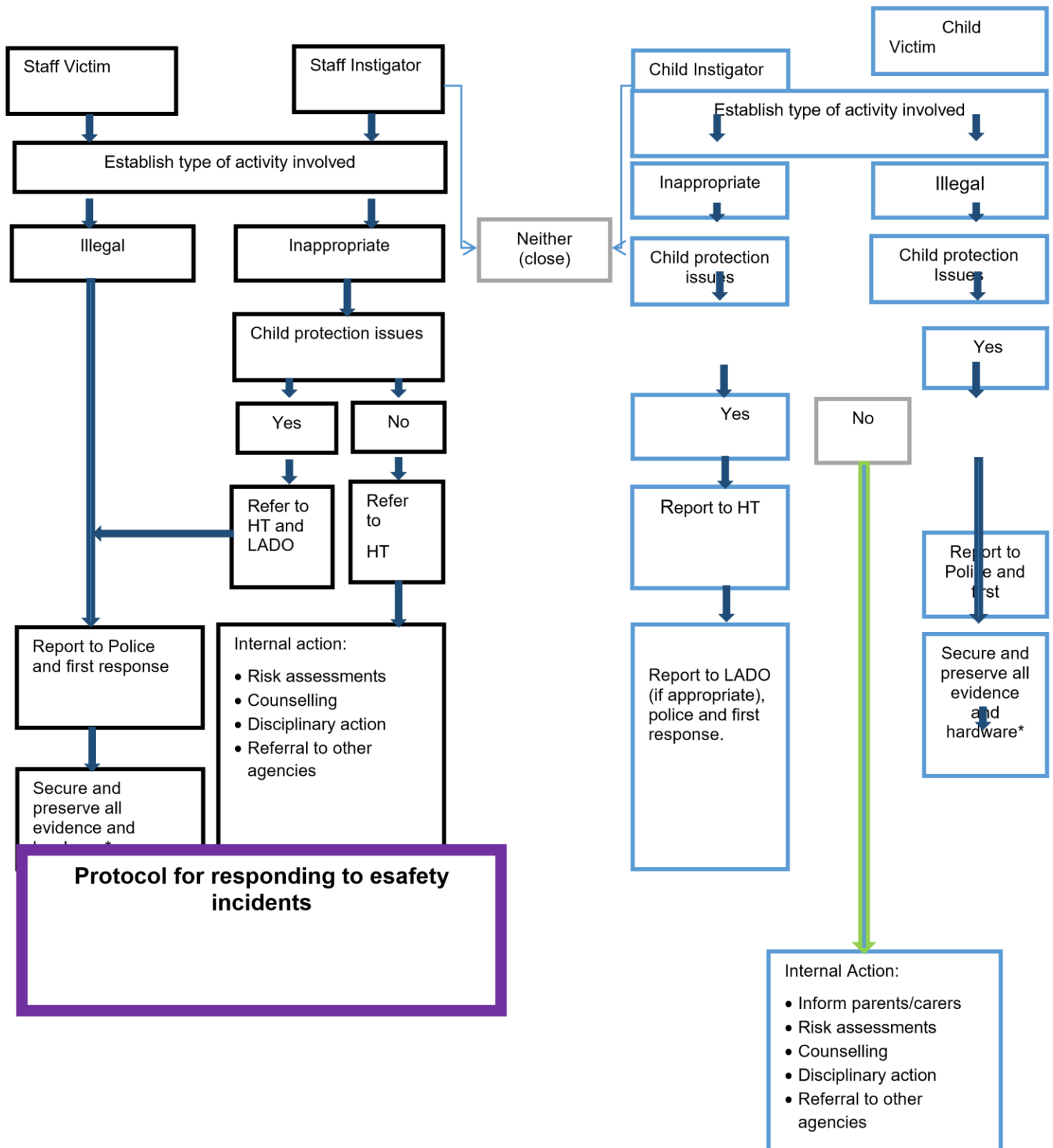


I have read the school social media policy and understand my responsibility to comply with requirements set down within it.

Full name:	
Relationship to School:	Pupil
Signature:	
Date:	

Appendix 5





E – SAFETY CONCERNS FORM

PARK BROW COMMUNITY SCHOOL

Name of person reporting incident:	
Date and time of incident:	
Date of Report:	
Computer/Item Location:	
Computer/laptop Number:	
Names of persons involved in incident:	
Details of the incident:	
Name of person incident reported to:	
Action Taken: (include dates)	
Outcome/Impact:	

Names and Signatures	
ROLE	SIGNATURE
Person Reporting Incident:	
E-Safety Curriculum Lead	
Safeguarding Coordinator	
Headteacher	

