Online Safety Policy

BROOKLANDS PRIMARY SCHOOL

Document Owner:	Headteacher
Issue Date/Approved by Govs:	September 2025
Revised Date:	
Version:	1.0
Review Frequency:	Annually
Date Approved by Governors:	

Aims

This policy takes into account the DfE statutory guidance 'Keeping Children Safe in Education', 'Early Years and Foundation Stage', 'Working Together to Safeguard Children'.

Within this policy, Brooklands Primary School aims to:

- Safeguard and protect all members of the school community online.
- Identify approaches to educate and raise awareness of online safety throughout the community.
- Enable all staff to work safely and responsibly, including in the delivery of remote learning, to role model positive behaviour online and to manage professional standards and practice when using technology.
- Identify clear procedures to use when responding to online safety concerns.

This school identifies that the issues classified within online safety are considerable, but can be broadly categorised into four areas of risk:

- Content: being exposed to illegal, inappropriate, or harmful content, for example: pornography, fake news (misinformation, disinformation & conspiracy theory), racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, and extremism
- Contact: being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.
- Conduct: online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying, and
- Commerce: risks such as online gambling, inappropriate advertising, phishing and or financial scams. If you feel pupils or staff are at risk, please report it to the Anti-Phishing Working Group (https://apwg.org/).

Scope of the Policy

This policy applies to all members of the school community (including staff, pupils, volunteers, parents/carers, visitors, community users) who have access to, and are users of, school ICT systems, both, in and out of the school.

The Education and Inspections Act 2006 empowers Head Teachers to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyberbullying, or other online safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data (see appendix for template policy). In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

The school will deal with such incidents within this policy and associated behaviour and antibullying policies and will, where known, inform parents/carers of incidents of inappropriate online safety behaviour that take place out of school.

Roles and Responsibilities

The following section outlines the online safety roles and responsibilities of individuals and groups within the school:

Governors:

Governors are responsible for the approval of the Online safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors C&P Committee receiving regular information about online safety incidents and monitoring reports. A member of the Governing Body has taken on the role of Online safety Governor. The role of the Online safety Governor will include the below actions:

- regular meetings with the online safety/computing Co-ordinator
- regular monitoring of online safety incident logs
- regular monitoring of filtering/change control logs

- reporting to relevant Governors' committee

Head Teacher:

- has a duty of care for ensuring the safety (including online safety) of members of the school community, though the day-to-day responsibility for online safety will be delegated to the Online safety Co-ordinator.
- as Designated Safeguarding Lead and the Deputy Safeguarding Lead are aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff.
- is responsible for ensuring that the Online safety Co-ordinator and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.
- will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role. This is to provide a support to those colleagues who take on important monitoring roles.
- will receive regular monitoring updates from the Online safety Co-ordinator.

Online safety Co-ordinator:

- takes day-to-day responsibility for online safety issues and has a leading role in establishing and reviewing the school safety policies/documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place
- provides training and advice for staff
- liaises with the relevant bodies, e.g. Flying High Trust, CEOP, CAS, Local Authority
- liaises with school technical staff
- receives reports of online safety incidents from LEAD IT and creates a log of incidents to inform future online safety developments
- meets regularly with Online safety Governor to discuss current issues, review incident logs and filtering/change control logs
- reports regularly to the Head Teacher.

Technical staff:

- ensure that the School's technical infrastructure is secure and is not open to misuse or malicious attack
- ensure that the School meets required online safety technical requirements and any Local Authority/other relevant body Online safety Policy/Guidance that may apply
- ensure that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed
- ensure filtering is applied and updated on a regular basis
- ensure that they keep up-to-date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- ensure that the use of the network/internet/remote access/email is regularly monitored in order that any misuse/attempted misuse can be reported to the Head Teacher for investigation/action/sanction
- ensure that monitoring software/systems are implemented and updated as agreed in school policies.

Teaching and Support Staff:

- ensure they have an up-to-date awareness of online safety matters and of the current school online safety policy and practices
- ensure that all children are taught about online safety, for 1 lesson per half term. This is to be recapped where appropriate in lessons.
- ensure they have read, understood and signed the Staff Acceptable Use Policy/Agreement
- ensure they report any suspected misuse or problem to the Head Teacher/Online safety Coordinator for investigation, action or sanction
- ensure all digital communications with pupils/parents/carers should be on a professional level and only carried out using official school systems
- ensure online safety issues are embedded in all aspects of the curriculum and other activities

- ensure pupils understand and follow the online safety and acceptable use policies
- ensure pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- ensure they monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities (where allowed) and implement current policies with regard to these devices
- ensure in lessons where internet use is pre-planned, pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

Child Protection/Safeguarding Designated Person:

This person is trained in online safety issues and aware of the potential for serious child protection/ safeguarding issues that may arise from the items below:

- sharing of personal data
- access to illegal/inappropriate materials
- inappropriate on-line contact with adults/strangers
- potential or actual incidents of grooming
- cyber-bullying

Pupils:

- are responsible for using the school digital technology systems in accordance with the Student/Pupil Acceptable Use agreement
- have a good 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 policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking/use of images and on cyber-bullying.
- should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the School's Online safety Policy covers their actions out of school, if related to their membership of the school.

Parents/Carers:

Parents/Carers play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website and information about national/local online safety campaigns/literature.

Parents and carers will be encouraged to support the school in promoting good online safety practice and to follow guidelines on the appropriate use of the below:

- digital and video images taken at school events
- access to parents' sections of the website, school blogs and other online school linked sites
- their children's personal devices in the school (where this is allowed)

3. Policy Statements

Education – pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in online safety is therefore an essential part of the school's online safety provision. Children and young people need the help and support of the school to recognise and avoid online safety risks and build their resilience.

Online safety is a focus in all areas of the curriculum and staff reinforce online safety messages across the curriculum. The online safety curriculum is broad, relevant and provides progression, with opportunities for creative activities and is provided in the following ways:

- a planned online safety curriculum is provided as part of Computing/RHSE/other lessons and is regularly revisited
- key online safety messages are reinforced as part of a planned programme of assemblies and tutorial/pastoral activities
- Pupils will be taught how to spot misinformation, disinformation and conspiracy theories.
- pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- pupils should be helped to understand the need for the pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school
- staff should act as good role models in their use of digital technologies, the internet and mobile devices
- in lessons where internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches
- where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.

Education – parents/carers

Some parents and carers may have a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring/regulation of the children's on-line behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

The school will therefore seek to provide information and awareness to parents and carers through the following:

- Curriculum activities
- Letters, newsletters, website
- Parents/Carers evenings/sessions
- High profile events/campaigns e.g. Safer Internet Day
- Reference to the relevant websites/publications e.g.
  https://ceop.police.uk/safety-centre/
  www.saferinternet.org.uk/
  http://www.childnet.com/parents-and-carers

Education & Training – Staff/Volunteers

It is essential that all staff receive online safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- A planned programme of formal online safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the online safety training needs of all staff will be carried out regularly.
- All new staff should receive online safety training as part of their induction programme, ensuring that they fully understand the school Online safety Policy and Acceptable Use Agreements.
- The Online safety Co-ordinator will receive regular updates through attendance at external training events (e.g. from Flying High Trust/Teaching School Alliance/other relevant organisations) and by reviewing guidance documents released by relevant organisations.
- This Online safety Policy and its updates will be presented to and discussed by staff in staff meetings.
- The Online safety Co-ordinator will provide advice/guidance/training to individuals as required.

Training – Governors

Governors should take part in online safety training/awareness sessions. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority/National Governors Association/or other relevant organisation
- Participation in school training/information sessions for staff or parents (this may include attendance at assemblies/lessons).

Technical – infrastructure / equipment, filtering and monitoring

Brooklands Primary School, through its partnership with the Flying High Trust will be responsible for ensuring that the school infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this Policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their online safety responsibilities:

- School technical systems will be managed in ways that ensure that the school meets recommended technical requirements.
- There will be regular reviews and audits of the safety and security of technical systems.
- Servers, wireless systems and cabling must be securely located and physical access restricted.
- All users will have clearly defined access rights to school technical systems and devices.
- The Flying High Trust are responsible for ensuring that software licence logs are accurate and up-to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations. (Inadequate licencing could cause the school to breach the Copyright Act which could result in fines or unexpected licensing costs).
- Internet access is filtered for all users. Content lists are regularly updated by LEAD IT and internet use is logged and regularly monitored. There is a clear process in place to deal with requests for filtering changes.
- School technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement.
- An appropriate system is in place for users to report any actual/potential technical incident/security breach to the relevant person as agreed.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, workstations, mobile devices etc. from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up-to-date virus software.
- An agreed policy is in place for the provision of temporary access of 'guests' (e.g. trainee teachers, supply teachers, visitors) on to the school systems.

Artificial Intelligence (AI) in Education – Guidance & Acceptable Use

Approved use of AI

While generative AI tools can streamline and expedite various written tasks, they do not substitute for the expertise and discretion of human professionals. Whatever tools or resources are used to produce plans, policies or documents, the quality and content of the final document remains the professional responsibility of the person who produced it. Any member of staff, trustee or local governor using an AI- generated plan, policy or document should only share the AI-generated content with other members of staff, trustees or local governors for use if they are confident of the accuracy of the information, as the content remains the professional responsibility of the person who produced it.

Permitted Uses of Microsoft Copilot (with a licensed account- connected to a work email address):

- Creating and refining lesson resources
- Summarising meeting notes or CPL readings
- Generating planning templates or policies
- Strategic school/partnership tasks
- Supporting administrative tasks
- Support the analysis of anonymised data.

Other Generative AI Systems (e.g., ChatGPT, Gemini, Claude)

- Use of third-party generative AI tools should be:
- For non-identifiable content only
- Never used to upload or generate content from personal, pupil, or school-sensitive data
- In alignment with DfE guidance, GDPR, data protection and FHP safeguarding procedures

Prohibited Use :

- Utilising work produced, without personalising, checking and ensuring accuracy.
- Resources development without human oversight.
- Use AI for formative or summative assessment without human moderation
- Use AI tools with pupils unless content has been pre-reviewed and quality assured.
- Illegal or harmful activities which deviates from our commitment to British Values and prevention of radicalisation.
- Inputting deliberately biased content, which may influence the training of the AI.
- Generate content to impersonate, bully or harass another person
- Generate explicit or offensive content
- Input offensive, discriminatory or inappropriate content as a prompt

Staff Training
All staff must exercise due diligence when integrating AI systems into educational settings, recognising the limitations and possible unintended consequences of these technologies. Clear protocols should be established for the development, review, and deployment of AI driven resources, ensuring that all content meets established standards for accuracy, appropriateness, and alignment with institutional values.

Ongoing professional development is essential to maintain staff awareness of emerging risks, evolving best practices, and the ethical landscape surrounding AI in education. The areas covered by the training will equip staff with the knowledge and skills needed to use AI safely and effectively in educational settings.

Educating pupils on AI

Educating students about artificial intelligence should encompass its capabilities, potential advantages, and inherent risks, with an emphasis on ethical considerations and the promotion of responsible usage. Instruction should include an overview of AI's operational principles, its diverse applications across multiple sectors, and awareness of issues such as bias, privacy concerns, and possible over-dependence. Fostering critical thinking and digital literacy is essential to equip learners to effectively navigate the complexities of AI.

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents/carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet, e.g. on social networking sites.
- In accordance with guidance from the Information Commissioner's Office, parents/carers are welcome to take videos and digital images of their own children at school events for their own personal use – in line with the School's policy - (as such use is not covered by the UK GDPR and the DPA 2018 plus DfE's DP Guidance). To respect everyone's privacy and in some cases protection, images of other parents' children should not be published/made publicly available on social networking sites, nor should parents/carers comment on any activities involving other pupils in the digital/video images, without the permission of the parents.
- Staff and volunteers are allowed to take digital/video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital/video images that pupils are appropriately dressed and 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.

- Photographs published on the website, or elsewhere, that include pupils will be selected carefully and will 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, unless express parental permission has been sought beforehand.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website (covered as part of an agreement signed by parents or carers at the start of the year).
- Pupil's work can only be published with the permission of the pupil and parents/carers.

Data Protection

Personal data will be recorded, processed, transferred and made available according to the UK GDPR and the DPA 2018 plus DfE's DP Guidance which states that 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.

The school must ensure the below:

- It will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.
- Every effort will be made to ensure that data held is accurate, up-to-date and that inaccuracies are corrected without unnecessary delay.
- All personal data will be fairly obtained in accordance with the 'Privacy Notice' and lawfully processed in accordance with the 'Conditions for Processing'.
- It has a Data Protection Policy.
- It is registered as a Data Controller for the purposes of the UK GDPR and the DPA 2018 plus DfE's DP Guidance (DPA).
- Responsible persons are appointed/identified - Senior Information Risk Officer (SIRO) and Information Asset Owners (IAOs).
- Risk assessments are carried out.
- It has clear and understood arrangements for the security, storage and transfer of personal data.
- Data subjects have rights of access and there are clear procedures for this to be obtained.
- There are clear and understood policies and routines for the deletion and disposal of data.
- There is a policy for reporting, logging, managing and recovering from information risk incidents.
- There are clear Data Protection clauses in all contracts where personal data may be passed to third parties.
- There are clear policies about the use of cloud storage/cloud computing which ensure that such data storage meets the requirements laid down by the Information Commissioner's Office.

Staff must ensure that they do the following:

- At all times take care to ensure the safe-keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only 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.

Transfer data using encryption and secure password protected devices:
When personal data is stored on any portable computer system, memory stick or any other removable media:

- the data must be encrypted and password protected
- the device must be password protected
- the device must offer approved virus and malware checking software

- the data must be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete.

Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. When using communication technologies, the school considers the following as good practice:

- The official school email service is currently through 'Microsoft Office 365'. 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).
- Users must immediately report, to the nominated person – in accordance with the school policy - the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- Any digital communication between staff and pupils or parents/carers (email, chat, etc.) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or social media must not be used for these communications.
- Pupils should be taught about online safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

The Use of Mobile Technology by Children

At Brooklands Primary School, we would prefer that no child brings a mobile phone to school. However, we recognise that some parents who allow their child to go home alone (in accordance with school policy) are reassured in the knowledge that their child has a mobile phone with them on their journey home. Therefore, in these circumstances only, we allow for selected children to bring a mobile phone to school.

The procedures are:

- A letter must be received by the parent outlining why they would like their child to bring a mobile phone to school
- The letter is stored in the school office (ensuring that it is dated and that it identifies the child's year group)
- If a phone is received by the school office and there is no parent letter, the office will call the parents immediately
- The office will ensure that the class teacher is aware of the arrangement for that child in case the parents have communicated only with the school office
- On a daily basis, the phone is handed to the class teacher by the child or parent
- The phone is stored securely in the classroom
- The phone is collected as the child leaves school at the end of the day by the child or parent

These arrangements are in place for children in Years 5 and 6. If a request is received for a child younger than this, it must be referred to the Head Teacher.

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

Social Media - Protecting Professional Identity

All schools, academies and local authorities have a duty of care to provide a safe learning environment for pupils and staff. Schools, Trusts and local authorities could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, cyberbully, discriminate on the grounds of sex, race or disability or who defame a third party may render the school, Trust or Local Authority liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the school through limiting access to personal information:

- Training to include acceptable use; social media risks; checking of settings; data protection; reporting issues.
- Clear reporting guidance, including responsibilities, procedures and sanctions
- Risk assessment, including legal risk

School staff should ensure the below:

- No reference should be made in social media to pupils, parents/carers or school staff.
- They do not engage in online discussion on personal matters relating to members of the school community.
- Personal opinions should not be attributed to the school or Local Authority.
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

This policy is in line with KCSIE 2025

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 1 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 tutor 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 makes available information on cyber-bullying to parents/carers so 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 report the incident and provide the relevant material to the police as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so.

Examining electronic devices

The headteacher, and any member of staff authorised to do so by the headteacher, can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

- Poses a risk to staff or pupils, and/or
- Is identified in the school rules as a banned item for which a search can be carried out, and/or
- Is evidence in relation to an offence

Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:

- Make an assessment of how urgent the search is, and consider the risk to other pupils and staff. If the search is not urgent, they will seek advice from the headteacher / DSL / appropriate staff member
- Explain to the pupil why they are being searched, how the search will happen, and give them the opportunity to ask questions about it
- Seek the pupil's co-operation

Authorised staff members may examine, and in exceptional circumstances erase, any data or files on an electronic device that they have confiscated where they believe there is a 'good reason' to do so.

When deciding whether there is a 'good reason' to examine data or files on an electronic device, the staff member should reasonably suspect that the device has, or could be used to:

- Cause harm, and/or
- Undermine the safe environment of the school or disrupt teaching, and/or
- Commit an offence

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL / headteacher / other member of the senior leadership team to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding if there is a good reason to erase data or files from a device, staff members will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

- They reasonably suspect that its continued existence is likely to cause harm to any person, and/or
- The pupil and/or the parent/carer refuses to delete the material themselves

If a staff member **suspects** a device **may** contain an indecent image of a child (also known as a nude or semi-nude image), they will:

- **Not** view the image
- Confiscate the device and report the incident to the DSL (or equivalent) immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on screening, searching and confiscation and the UK Council for Internet Safety (UKCIS) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

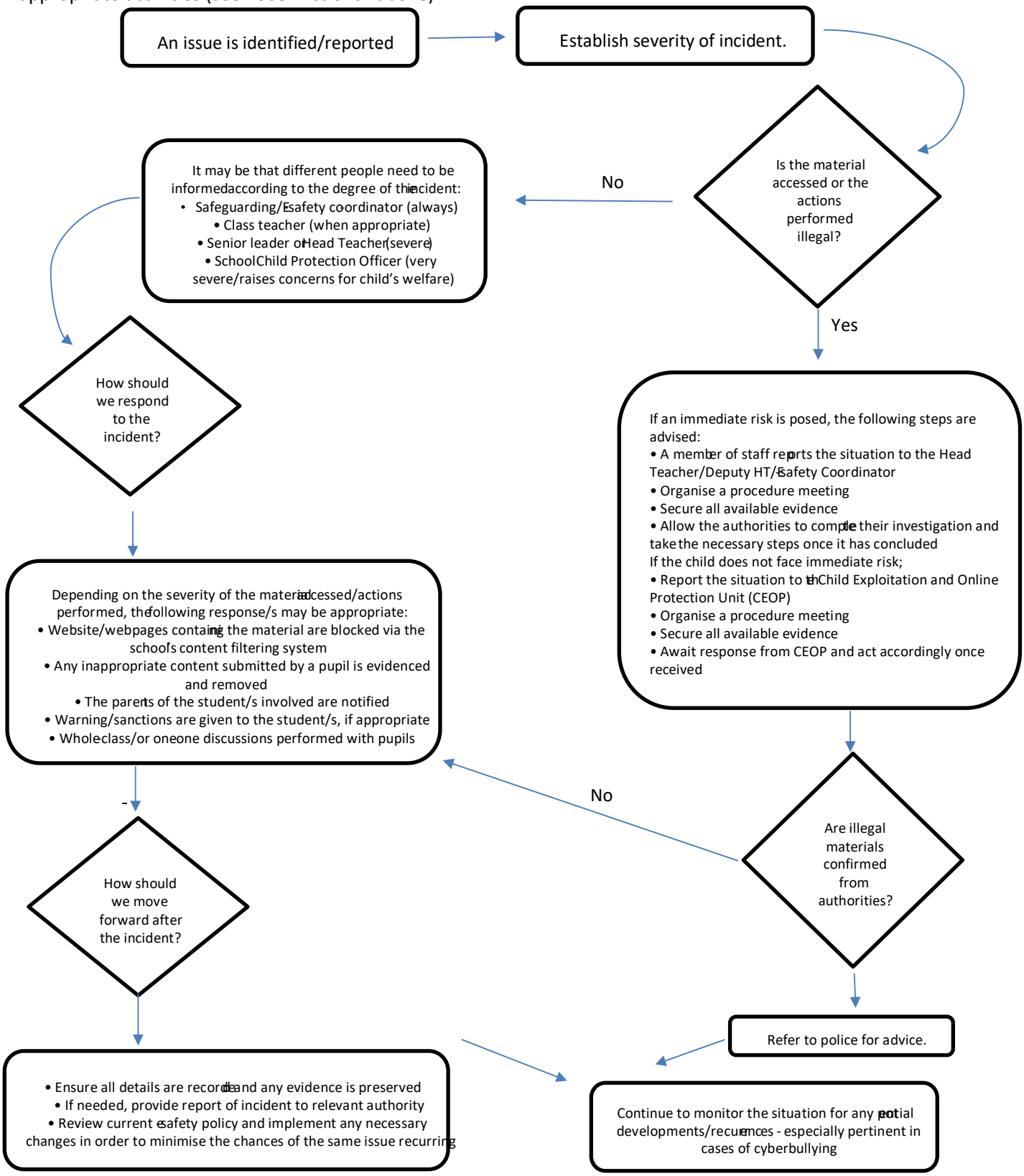
Any searching of pupils will be carried out in line with:

- The DfE's latest guidance on searching, screening and confiscation
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- Our behaviour policy

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

Responding to incidents of misuse

This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities (see "User Actions" above).



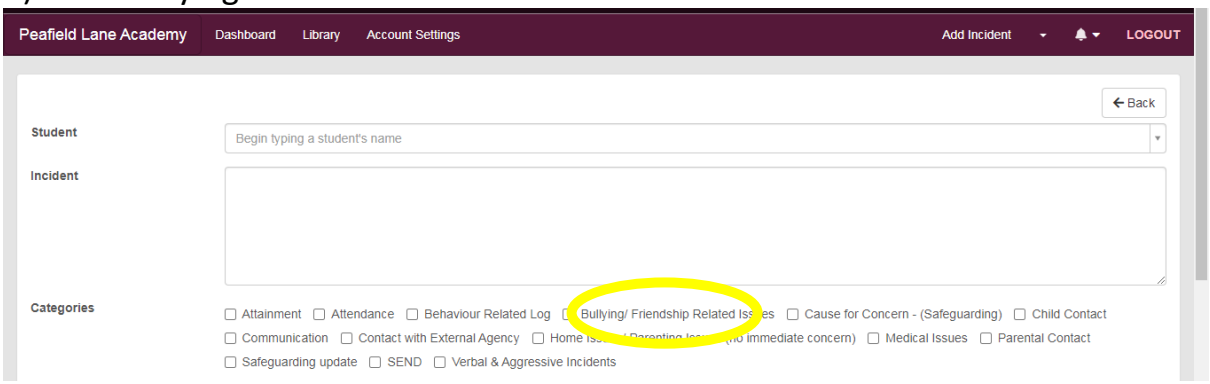
Other Incidents

All incidents, regardless of severity should also be reported through CPOMs. The procedure for this is below. If staff do not have access to CPOMs, or the incident is being recorded by a visitor, they should contact a member of the DSL who will report it using their online account.

Reporting Online safety concerns.

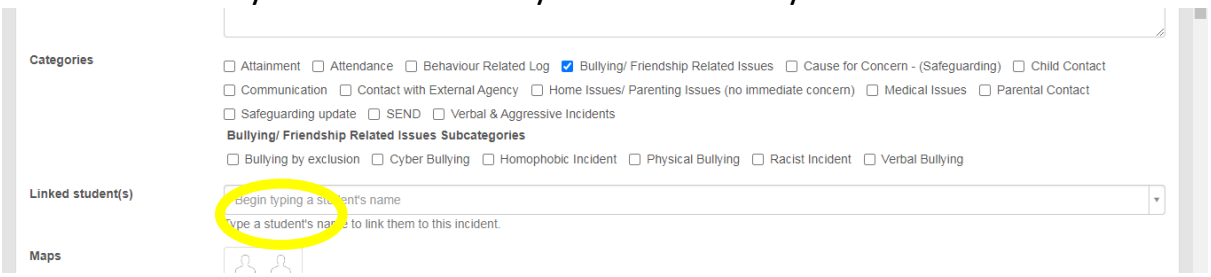
1) Open up CPOMs and click “add incident”

2) Click bullying



3) This will load ‘bullying subcategories,’ after click cyber bullying.

4) Record the incident as you would normally. Please ensure you include as much detail as possible.



No matter how small it may seem, please ensure it is recorded. It allows us to keep track and recognise patterns.

More serious incidents.

It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow school policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

In the event of suspicion, all steps in this procedure should be followed:

- Have more than one senior member of staff involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary, can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the url of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation.

These maybe printed, signed and attached to the form (except in the case of images of child sexual abuse – see below).

- Once this has been completed and fully investigated, the group will need to judge whether this concern has substance or not. If it does, then appropriate action will be required and could include the following:
- Internal response or discipline procedures
- Involvement by Local Authority or national/local organisation (as relevant)
- Police involvement and/or action

If content being reviewed includes images of child abuse then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:

- incidents of 'grooming' behaviour
- the sending of obscene materials to a child
- adult material which potentially breaches the Obscene Publications Act
- criminally racist material
- other criminal conduct, activity or materials

Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.

It is important that all of the above steps are taken as they will provide an evidence trail for the school and possibly the police, and demonstrate that visits to these sites were carried out for child protection purposes. The completed form should be retained by the group for evidence and reference purposes.

School Actions & Sanctions

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour/disciplinary procedures.

Appendix 1: Acceptable use of the internet: agreement for staff, governors and visitors

Brooklands Primary School

Staff, Governor and Visitor Acceptable Use Agreement

ICT and the related technologies such as email, the internet and mobile devices are an expected part of our working life in school. This policy is designed to ensure all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this policy and adhere at all times to its contents.

- I appreciate that ICT includes a wide range of systems and devices including mobile phones, PDAs, digital cameras, email, social networking and may include personal ICT devices when used for school business.
- I understand that it is a criminal offence to use a school ICT system for a purpose not permitted by its owner.
- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities.
- I understand that I am responsible for all activities carried out under my user name.
- I will only use the school email, internet, intranet or any related technologies for professional purposes.
- I will ensure that personal data is kept secure and used appropriately, whether in school, taken out of school or used remotely when authorised by the Head Teacher or governing body.
- I will not install any hardware or software without permission.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- I will respect copyright and intellectual property rights.
- Images of pupils and/or staff will only be taken, stored and used for professional purposes in line with school policy and with consent of the parent, carer or staff member. Images will not be distributed outside the school network without permission.
- I will ensure that my online activity both in school and outside school will not bring my professional role into disrepute.
- I will ensure that all electronic communications with parents, pupils and staff are compatible with my professional role and that messages cannot be misunderstood or misinterpreted.
- I will support the school's online safety policy and help pupils to be safe.
- I will report any incidents of concern regarding children's safety to the Designated Safeguarding Leads or the Head Teacher.
- I understand that sanctions for disregarding any of the above will be in line with the school's disciplinary procedures and serious infringements may be referred to the police.

User Signature
I agree to follow the agreement and support the safe use of ICT throughout the school

Full Name: _____

Job Title: _____

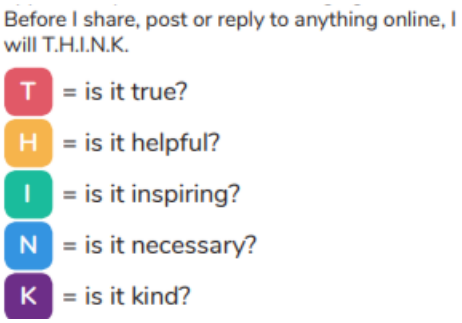
Signature_____ Date_____

Appendix 2: Acceptable use agreement for KS2 children

Brooklands Primary School

KS2 Pupil Acceptable Use Agreement These rules will keep me safe and help me to be fair to others.

- I will only use the school's computers for schoolwork and homework.
- I will take care of the computer and other equipment.
- I will keep my logins and passwords secure.
- I will not bring files into school without permission or upload inappropriate material to my workspace.
- I am aware that some games have age restrictions and I should respect this.
- I will not attempt to visit Internet sites that are not appropriate.
- I will only e-mail people I know, or people who a responsible adult has approved.
- The messages I send, or information I upload, will always be polite and sensible.
- I will not open an attachment, or download a file, unless I know and trust the person who has sent it.
- I will not give my home address, phone number, send a photograph or video, or give any other personal information that could be used to identify me, my family or my friends, unless a trusted adult has given permission.
- 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 will never arrange to meet someone I have only ever previously met on the Internet.
- If I see anything I am unhappy with or I receive a message I do not like, I will not respond to it but I will show a teacher / responsible adult.



I have read and understand these rules and agree to them.

Name:_____

Class:_____

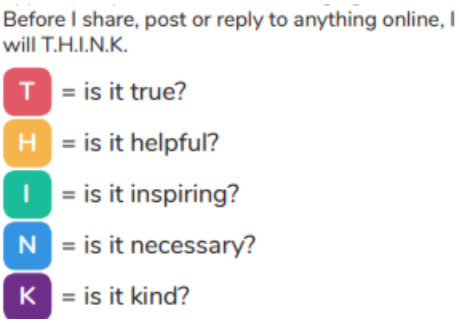
Appendix 3: Acceptable use agreement for KS1 children

Brooklands Primary School

KS1 Pupil Acceptable Use Agreement

This is how we stay safe when we use computers and devices:

- I will ask a teacher or suitable adult if I want to use the computers or device.
- I will only use activities that a teacher or suitable adult has told or allowed me to use.
- I will take care of the computer and other equipment.
- I will ask for help from a teacher or suitable adult if I am not sure what to do or if I think I have done something wrong.
- I will tell a teacher or suitable adult if I see something that upsets me on the screen.
- I will not give out any personal information like my name, age, home address or school.
- Use devices sensibly for school work
- Keep my passwords and logins a secret.



I have read and understand these rules and agree to them.

Name:_____

Class:_____

Appendix 3: Acceptable use agreement for EYFS children

Brooklands Primary School

EYFS Pupil Acceptable Use Agreement