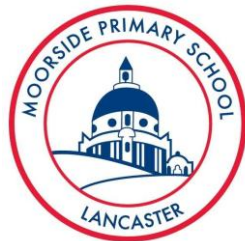


Moorside Primary School		
Document Name	Online Safety Policy	
Date	September 2026 Next Review: September 2027	
Version	4	
Audience	Staff, Governors, Volunteers, Parents, Website	
Approved by	The Governing Body, 10 th September 2026	

Background and Scope of the Policy

This policy applies to all members of the school community (including staff, pupils, volunteers, parents and carers, visitors, community users) who have access to and are users of school digital systems, both in and out of the school. It also applies to the use of personal digital technology on the school site (where allowed)

This Online Safety Policy is one of a number of policies which form part of the school's approach to safeguarding. Other documents which are specifically related to it are the:

- Child Protection and Safeguarding Policy
- the school's statements about Responsible Computer Use displayed in school for pupils
- the staff 'Acceptable Use Policy'.
- use of IT agreements signed by pupils
- Monitoring and Filtering Policy

Through this policy, we aim to set out:

- how technology can enhance learning and describe the range of technology used in school
- how we balance security measures with the need for children to learn effectively
- how we educate pupils to recognize the risks associated with technology and how to deal with them

The policy also sets out how we work with pupils to educate them about opportunities and risks posed by online activity and how the school responds when inappropriate use has been made of technology.

Where online safety concerns or incidents occur both in school or outside school and are known to the school, Moorside Primary School will respond in line with this policy and related procedures, including the school's Safeguarding, Behaviour and Anti-Bullying policies.

Responsibilities

Online safety is a shared responsibility. All members of the school community are expected to model safe, responsible behaviour, report concerns promptly and learn from incidents and good practice. The roles below clarify accountability.

Governors

Governors are responsible for ensuring that there is an Online Safety Policy and that:

- all staff undergo safeguarding and child protection training (including online safety which, amongst other things, includes an understanding of the expectations, applicable roles and responsibilities in relation to filtering and monitoring – at induction and regularly updated)
- children be taught about safeguarding, including in relation to online safety
- the school works in line with the DfE Filtering and Monitoring Standards and discuss with IT staff and service providers what more needs to be done to support the school in meeting this standard

At Moorside, the Safeguarding Governor takes on responsibility for online safety and monitoring and filtering. The role of the Online Safety Governor will include:

- regular meetings with the Online Safety Lead/DSL
- attendance at School Council meetings where Online Safety is discussed or receive information from them
- regular monitoring of online safety incident logs
- regular monitoring of filtering logs
- reporting to relevant governors' meetings

Headteacher and Senior Leaders

The Headteacher, along with senior leaders and the DSL team set the culture and ensure that systems are effective

- In conjunction with the DSL team and the Online Safety Lead, the Headteacher is responsible for the development of policy and practice
- The Headteacher also has a duty of care for ensuring the safety (including online safety) of members of the school community on a day-to-day basis (ie incidents arising out of any breaches of the filtering system). The Headteacher will liaise with the Online Safety Lead and technician about issues which may arise.
- The Headteacher is responsible for liaising with the provider which monitors the effectiveness of the school's filtering system.
- The Headteacher and DSL should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff. (see flow chart on dealing with online safety incidents – included in a later section – “Responding to incidents of misuse” and relevant *Local Authority* disciplinary procedures).
- The Headteacher and Senior Leaders are responsible for ensuring that the Online Safety Lead and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant. This includes: includes an understanding of the expectations, applicable roles and responsibilities in relation to filtering and monitoring.
- Put in place appropriate oversight and support for internal monitoring activity.
- Ensure that children are taught about how to keep themselves and others safe online, recognising that effective education will be tailored to the specific needs and vulnerabilities of individual children
- Establish and receive regular online safety reports and act on emerging risks and themes.

Online Safety Champion/Lead

At Moorside the Online Safety Lead is the Headteacher. Their responsibility is to liaise with the Computing Curriculum Leader, IT Technician and the DSL Team and through this work advise colleagues about aspects of teaching. They work in conjunction with the DSL team to promote safeguarding and respond when issues arise.

- the lead DSL and Online Safety Lead meet with the pupil group (School Council) who report on online safety issues
- they have a leading role in establishing and reviewing the school online safety curriculum provision
- Work with curriculum leads to map, embed and evaluate online safety education
- provide training and advice for staff
- liaises with school technical staff
- they receive reports and handle with the DSL issues which have been identified and adapt teaching and provision accordingly
- liaise with the Online Safety Governor to discuss current issues
- reports to Senior Leadership Team if issues arise relating to use of technology in school

IT service provider / IT Technician

The IT provider supports leaders and the DSL to meet DfE filtering, monitoring and technical standards.

The IT provider will:

- Maintain secure infrastructure and managed user access.
- Implement, maintain and update filtering and monitoring; provide reports; act on alerts and concerns.
- Support procurement, risk identification, reviews and checks with SLT/DSL.
- Monitor systems for misuse and report concerns promptly to the Headteacher
- Follow the school's Online Safety and Technical Security policies and keep technical knowledge current

Teaching and Support Staff

Are responsible for ensuring that:

- they follow the Online Safety Policy, the Safeguarding/Child Protection Policy and work in accordance with Acceptable USE of IT Agreement
- they use only school-approved digital services and AI tools; protect data, apply UK GDPR, and verify AI outputs for accuracy/bias before use
- they have an up to date awareness of online safety matters and of the current school safety policy and practices
- they have read, understood and signed the staff acceptable use agreement
- they challenge harmful online behaviour and report concerns promptly
- they report any suspected misuse or problem to the Headteacher for investigation and appropriate action
- all digital communications with pupils and parents/carers should be on a professional level and only carried out using official school systems
- online safety issues are embedded in all aspects of the curriculum and other activities
- pupils understand and follow the Online Safety Policy and acceptable use agreements
- pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations (at age-appropriate levels)

- 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
- 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
- computer use is carried in line with the Monitoring and Filtering Policy

Designated Safeguarding Lead

Should be trained in online safety issues and be aware of the potential for serious child protection/safeguarding issues to arise from:

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

The DSL will:

- Lead safeguarding, including online safety, with clear responsibilities in their job description
- Maintain up-to-date knowledge of online risks, filtering/monitoring and cyber security
- Coordinate and record online safety concerns and incidents, escalating and referring in line with safeguarding procedures

Online Safety Group

At Moorside our 'Online Safety Group' comprises of:

- Headteacher/Online Safety Lead
- Computing Curriculum Lead
- PSHE Leader
- DSL

It involves pupils through taking feedback from the School Council which gathers pupil views, suggestions and concerns.

Members of the Online Safety Group will assist the school leadership with:

- monitoring of the school filtering policy and requests for filtering changes
- mapping and reviewing the online safety/digital curricular provision – ensuring relevance, breadth and progression
- monitoring network/internet/filtering/incident logs
- consulting stakeholders – including parents/carers and the pupils about the online safety provision

Pupils:

- are responsible for using the school digital technology systems in accordance with the student/pupil acceptable use agreement
- develop 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 online-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
- report concerns and how to get help

External Stakeholders

Families, the wider community and external agencies play a vital role in supporting the online safety education and wellbeing of learners. The school recognises that parents and carers may have limited awareness of online risks, and that many external bodies can enhance the school's safeguarding approach. The school therefore works actively to build strong partnerships, share key messages, and ensure that families and the wider community are equipped to help keep children safe online.

Moorside School will seek to provide information and awareness to parents and carers through:

- curriculum activities
- letters, newsletters and the school web-site,
- workshop sessions
- high profile events/campaigns e.g. Safer Internet Day
- reference to the relevant web sites/publications e.g. [swgfl.org.uk](http://www.swgfl.org.uk), www.saferinternet.org.uk/, <http://www.childnet.com/parents-and-carers> (see appendix for further links/resources)

Parents/carers will be encouraged to reinforce key messages and support safe use of personal devices.

Community Users

Community users who access school systems are asked to sign the school's Acceptable Use Agreement.

Teaching about Online Safety

Why the internet and digital communications are important

The internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide pupils with quality internet access as part of their learning experience. Children are taught how to use the internet effectively, critically and safely in specific computing lessons. They also make use of it as a tool for research within other subjects.

Teaching about online safety

The content of our teaching is based on the SWGfL (Project Evolve and the PSHE Association programmes) Learning is age-appropriate and builds on prior learning. There are a number of approaches to our teaching about online safety

1. Explicit teaching about online safety takes place **through dedicated sessions**. These include:
 - computing lessons which explore different issues and allow children to apply their learning in a range of contexts
 - PSHE lessons

-Kidsafe which addresses online safety at age appropriate levels as the children move through school
-assemblies

2. Children also learn about **keeping safe online through the use of technology in other subjects**. For example, they are given reminders within other subjects when the internet is being used for a range of purposes; within these, children are taught to evaluate what they see and to be critically aware of content and materials and an environment should be created where they feel comfortable to discuss issues arising from the materials.
3. Other aspects to the teaching of safety online
 - pupils are 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 are 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 search the internet on a given theme, staff should be vigilant in monitoring the content of the websites the pupils visit.

Enhancing learning through the use of the internet

Internet access is an essential aspect of a school in the 21st century. The level of access is tailored to the needs of the users across the school and includes filtering appropriate to the age of pupils. Levels of staff access are different to those of pupils, but this higher level of access is restricted to computers used by staff.

At times, pupils will be taught specific skills for searching the internet effectively. At other times, they will use the internet as tool to enhance learning in other subjects.

- pupils will be taught what internet use is acceptable and what is not and given clear objectives for internet use.
- pupils will be educated in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation
- pupils will be shown how to publish and present information to a wider audience in an appropriate way.

Pupils will be taught how to evaluate internet content

The school makes use of 'Fortinet' as a system for filtering content. Although it is filtered, the system does not provide a complete block as this is seen as limiting pupil ability to learn about appropriate use.

- the school will ensure that the use of internet-derived materials by staff and pupils complies with copyright law.
- pupils will be taught the importance of cross-checking information before accepting its accuracy.
- pupils will be taught how to report unpleasant internet content to teachers or to the Online Safety Lead.
- they will be taught that not all content is true and could be generated by AI, whilst some may contain bias or discrimination

Use of Artificial Intelligence

Generative AI (Gen AI) is developing rapidly and its use in education is increasing. At Moorside Primary School, AI is typically used in two areas: teacher support (prepare resources, research) and school operations. All use must be safe, ethical and responsible. Whilst pupils may not use it explicitly, it is understood that AI underpins many IT functions.

We recognise that Gen AI can introduce risks. These risks can be reduced through our existing safeguarding, data protection and technical security arrangements, and by updating procedures where needed. Safeguarding of learners and staff remains central to our approach.

KCSIE 2026 recognises that learners may be subject to harmful online interaction with other users or generative AI applications that simulate these.

The school will:

- Support appropriate use of AI to enhance learning and teaching, improve outcomes, streamline administration and reduce workload. Staff remain professionally responsible and accountable for any work supported by AI.
- Comply with relevant law and guidance, including Keeping Children Safe in Education (KCSIE) and UK GDPR.
- Provide training and guidance for staff and governors on the benefits, risks and safe use of AI, and identify further development needs.
- Teach about AI through the curriculum where appropriate, helping learners understand how Gen AI works, its benefits and limitations, and its ethical and social impacts.
-

Safe use, data protection and security

The school will:

- Protect personal and sensitive data. Staff must not enter personally identifiable or sensitive information into AI tools. Where AI is used, staff should use anonymised data only.
- Require UK GDPR compliance. Staff must ensure any AI tool used meets data protection and security requirements before use.
- Approve tools and accounts. Only school-approved AI tools may be used for schoolwork, and staff should use school-provided AI accounts where available to support oversight and reduce risk.
- Safeguard sensitive information. Internal documents, strategic plans or other sensitive material must not be entered into third-party AI tools unless the tool and purpose have been explicitly approved.

Quality, fairness and integrity

The school will:

- Maintain human oversight - AI may support work but must not replace professional judgement—especially in decisions that affect people. AI outputs must be checked for accuracy before sharing or publishing.

- Promote transparency - Where AI has materially supported an output (e.g. documents, presentations, communications), staff should make this clear where appropriate.
- Address bias and discrimination - We recognise AI outputs may reflect bias. The school will use appropriate safeguards, review processes and procurement checks to prioritise fairness and safety.

Technical Security

The school takes steps to ensure that its technical infrastructure is secure, reliable and well managed and meets its statutory requirements.

The school ensures that:

- access to systems and data is controlled through appropriate authentication and permissions
- devices, networks and systems are protected through secure configuration, patching and malware protection
- backups and recovery arrangements are in place to reduce the impact of system failure or attack
- incidents and weaknesses are reported, recorded and used to inform improvement
- responsibilities for technical security are clearly defined and supported by appropriate expertise
- systems are regularly reviewed and tested, meet statutory requirements and address emerging threats.

Cyber Security

The school recognises cyber security as a leadership and governance responsibility and takes steps to reduce the risk and impact of cyber incidents. (KCSIE 2026 refers to the [DfE Cyber Security Standards](#) and recognises cyber security as a safeguarding issue).

The school ensures that:

- a cyber security approach is in place to prevent, detect, respond to and recover from cyber threats
- senior leaders and governors understand cyber risks and their safeguarding implications receive appropriate assurance
- staff and learners are educated/trained to recognise and report cyber security concerns
- business continuity and incident response arrangements are maintained and reviewed
- cyber security arrangements are kept under regular review and updated in line with emerging risks.

Data Protection

The school is committed to protecting personal data and complying with data protection legislation. [The Data \(Use and Access\) Act 2025](#) makes additional requirements on schools – particularly that online services accessed by pupils meet higher protection standards)

The school ensures that:

- personal data is processed lawfully, fairly and transparently
- a Data Protection Officer (DPO) is appointed and appropriate governance arrangements are in place
- all staff receive regular training to ensure they are aware of their responsibilities and can respond appropriately to data protection incidents.

- systems are in place to respond effectively to Freedom of Information and Subject Access Requests
- Data Protection Impact Assessments have been conducted on existing and planned use of software and systems.
- privacy notices explain how data is used and how individual rights can be exercised
- data is stored, shared and disposed of securely
- data breaches are reported and managed in line with legal requirements
- data protection is embedded across safeguarding, teaching, learning and administration

Review

Arrangements for filtering, monitoring, technical/cyber security and data protection are reviewed regularly and updated to reflect:

- changes in technology
- emerging safeguarding risks
- national guidance and statutory expectations

Device Management

The school manages the use of digital devices in a way that supports safeguarding, learning and responsible behaviour. This reflects KCSIE's requirement for a clear mobile / smart technology policy and explicitly links device use to behaviour, safeguarding and education.

Authorising internet access

At Key Stage 1, access to the Internet will be by adult demonstration with directly supervised access to specific, approved on-line materials. At Key stage 2, pupils have greater freedom to search the internet, but they should do this according to guidelines set by the teacher. Where internet use is likely to involve the need to access content which may trigger the filtering system, then a discussion must take place with the Headteacher to establish the reasons for the search and so that the filtering company can be notified.

If computers are being used outside of lesson time eg during a break or after-school club, children should only be accessing sites which are designated as safe and should be supervised in the same way as if they were in a lesson, with regular checks being made to monitor their activity.

The school ensures that:

- expectations for the use of school-owned and personal devices are clearly defined and communicated
- device use is consistent with safeguarding, behaviour, data protection and acceptable use policies
- appropriate technical and procedural controls are in place to support safe use
- staff, learners and visitors have been trained/educated/informed and understand their responsibilities when using devices on school premises or systems
- education on the safe and responsible use of devices forms part of the school's online safety education
- as part of the behaviour policy, and in line with the [DfE statutory guidance](#), the school prohibits for learners the use of mobile phones and other smart technology with similar functionality to mobile phones throughout the school day, including during lessons, the time between lessons, breaktimes and lunchtime.

Training

Staff

Adults in school receive training in line with their responsibilities. 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.
- all new staff should receive online safety training as part of their induction programme, ensuring that they fully understand the school safety policy and acceptable use agreements.
- the Online Safety Lead (or other nominated person) will receive regular updates through attendance at external training events 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 be circulated electronically and be stored in an accessible place on a drive accessible by staff.
- the Online Safety Lead (or other nominated person) will provide advice/guidance/training to individuals as required.

Governors - Training

- Attendance at training provided by the Local Authority/National Governors Association/or other relevant organisation (e.g. SWGfL).
- Participation in school training/information sessions for staff or parents

Public Online Communications

The school uses public online communications to inform, celebrate success and engage with the wider community, while managing associated risks. It supports KCSIE expectations around professional boundaries and staff conduct online, addresses reputational and safeguarding risk from public platforms while reinforcing parental engagement and transparency. It has considered the risks of AI manipulation of images as highlighted in the UK Online Harms Early Warning group guidance. [Protecting your setting's images from AI manipulation and abuse](#). To reduce the risk of illegal manipulation of publicly available images of staff and learners, the school has procedures in place to control how those images are shared online.

Two main media are used. These are the official school website and the school's official Facebook page. A number of basic rules will be followed to ensure that content is appropriate and does not expose staff or pupils to undue risk:

- public online communications are appropriate, accurate and well-managed
- public communications from or regarding the school are monitored and addressed where appropriate
- staff or pupil personal contact information will not be published. The contact details given online should be the school office.
- the number of staff who can physically upload material is restricted.
- the headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate.
- photographs that include pupils will be selected carefully and should never include any pupils whose parents who not given consent.

- photographs of pupils will be taken in such a way that a full view of their face is not visible or be taken such a distance that it becomes pixelated upon enlargement
- a pupil's full name will not be used anywhere on a school website or other on-line space, particularly in association with photographs.
- written permission from parents or carers will be obtained before photographs of pupils are published
- work can only be published with the permission of the pupil and parents/carers.
- parents are clearly informed of the school policy on image taking and publishing, both on school and independent electronic repositories.

Filtering and Monitoring

The school has appropriate filtering and monitoring systems in place to help protect users from illegal, inappropriate and harmful online content and activity, in line with statutory guidance. (e.g., DfE Technical Standards, DfE Generative AI: product safety standards; KCSIE) and best practice guidance (e.g., UKSIC Appropriate Filtering and Monitoring). The leadership team and relevant staff have an awareness and understanding of the provisions in place and manage them effectively and know how to escalate concerns when identified.

The school ensures that:

- filtering and monitoring arrangements are safeguarding-led, proportionate and regularly reviewed
- filtering blocks illegal content and provides age-appropriate and role-appropriate access
- monitoring supports the rapid identification of safeguarding concerns and enables timely intervention
- all school-owned devices are subject to filtering and monitoring, including when used off-site
- staff and learners understand that filtering and monitoring are in place, why they are needed, and how concerns are escalated
- where the use of personal devices (by adults) is allowed, users understand that their use is filtered and monitored by the school.
- where Generative AI products are used they must effectively and reliably prevent users from accessing harmful or inappropriate content and filtering mechanisms should be embedded within these products
- the technical limitations of the filtering system are understood, including whether the solution can monitor and filter real-time, dynamic, personalised or AI generated content

Children are only permitted to use computer equipment in the presence of adults. If they are using the internet, it should be to access a specific programme or APP, or to search on a given topic. Further details about the school's approach to monitoring and filtering can be found in the Monitoring and Filtering Policy.

Reporting and Responding

Moorside Primary School is committed to creating a culture where all members of the community feel confident, safe, and supported in reporting online safety concerns. In line with *Keeping Children Safe in Education (KCSIE)*, the school recognises that online risks may occur in school or outside school and may affect children in any setting. Reporting routes must therefore be clear, accessible, inclusive, and consistently understood by all.

Moorside Primary School recognises national findings, including the [Ofsted Review of Sexual Abuse in Schools and Colleges \(2021\)](#), which highlight that children may not always feel able to report. The school assumes that harmful online behaviours may be occurring, even where none have been disclosed, and

responds by maintaining strong systems for reporting, analysing, and addressing concerns. KCSIE suggests that staff should have a professional curiosity and speak to the designated safeguarding lead (or a deputy) if they have concerns about a child

Reporting Concerns

Moorside Primary School will ensure that:

- Clear, accessible reporting routes are in place for all members of the school community, including pupils, staff, governors, parents/carers, and volunteers.
- Reporting processes are fully aligned with safeguarding procedures, including the child protection, whistleblowing, managing allegations and complaints policies.
- Multiple reporting options are available, such as speaking with the Designated Safeguarding Lead, Headteacher, Trusted Adult (for children), email contact, or in-person disclosures.
- Reporting routes are well publicised through induction, assemblies, posters, the school website, and digital platforms.
- All users understand that any online safety concern must be reported, including those relating to harmful or illegal behaviour, sexual harassment, bullying, discrimination, grooming, or self-generated sexual imagery.

Responding to Concerns

Moorside Primary School will ensure that:

- Reports are acknowledged and responded to promptly, considering the safety and wellbeing of the person reporting.
- The DSL, Online Safety Lead, and senior leaders have the training and skills needed to recognise, assess, and manage online safety risks.
- Where a report indicates possible illegal activity or serious harm, it is escalated immediately through safeguarding procedures. Examples include (but are not limited to):
 - Child sexual abuse material (CSAM)
 - Non-consensual or self-generated images
 - Grooming, exploitation, or sexual harassment
 - Terrorism or extremism
 - Hate crime, fraud, extortion, stalking
 - Cyber offences under the Computer Misuse Act
 - Sale of illegal substances or goods
- Where concerns do not involve suspected illegal activity, devices may be checked using a safe, controlled, and documented process involving senior staff and a designated review device.
- AI-supported monitoring systems, where used, are subject to human oversight to ensure contextual understanding.
- Users who report concerns receive reassurance, appropriate support, and feedback on the outcome.

Recording and Monitoring

Primary School School will:

- Maintain a secure and confidential record of all incidents, including actions, decisions, and follow-up.
- Ensure reports are audited and analysed regularly to identify emerging trends, patterns of concern, and the effectiveness of responses.
- Provide anonymised summaries of trends and learning to:
 - The Online Safety Group
 - Senior leaders

- Governors (via safeguarding reports)

Oversight and Review

- Senior leaders, the Designated Safeguarding Lead (DSL), technical staff and governors have clear roles and responsibilities
- Governors will review the DfE Filtering and Monitoring Standards and discuss with IT staff and service providers what needs to be done to support the school in meeting this standard.
- filtering and monitoring effectiveness is reviewed at least annually, and following significant changes or incidents. (e.g., using [Testfiltering](#)). Reviews will be carried out by the SLT member responsible for filtering and monitoring, with the support of the school's designated safeguarding lead and IT support. The review will include checks that filtering is working appropriately on all internet-connected devices in all relevant locations. Record of these checks will be kept and will include: when checks were conducted; which devices and environments were tested, issues identified and actions taken.
- log reports provide actionable information for safeguarding decisions.
- no system is relied upon in isolation; reporting routes and professional judgement remain central

Evaluation and Review

The policy will be reviewed at least annually or when significant changes in technology occur. We will consider the number of complaints received, the occurrence of inappropriate materials, the receipt of any offensive messages and computer or phone misuse by staff or pupils.

Appendix 1

RESOURCES

www.thinkuknow.co.uk KS2

www.hecctorsworld.com KS1

www.digizen.org/cyberbullying

www.teachernet.gov.uk

www.thinkuknow.co.uk/teachers

www.childnet.com

www.becta.org.uk/schools

Appendix 2 – see below for responding to an incident

