Inkpen Primary School

Aiming high

Online Safety Policy

Date Created	December 2022
Date Modified & Agreed	December 2025
Revision Due	December 2027

Change History

Version	Date	Description
3	Dec 2025	Updated to reflect changes made to KCSiE 2025

Linked Policies	Safeguarding Policy

Signatures:

Headteacher:

FRANCES BUCK

Chair of Governors:

SUSAN R. SIM

Online Safety Policy

1 Policy Status and Scope

This is a statutory policy. It applies to all members of the school community, including staff, pupils, governors, volunteers, contractors, and visitors, both on and off the school premises when representing the school or using school-provided technology. It forms part of the school's wider safeguarding and child protection framework and should be read in conjunction with related policies, including Safeguarding and Child Protection, Behaviour, Anti-Bullying, Data Protection, and Acceptable Use Agreements.

2.0 Policy Statement and Aims

2.1 Policy Statement

Inkpen Primary School is committed to safeguarding and promoting the welfare of all children and young people in our care, including their safety and wellbeing in the digital environment. We recognise our statutory duty under the Education Act 2002 (Section 175), Keeping Children Safe in Education (KCSIE) 2025, and other relevant legislation to protect pupils from harm, including risks associated with online activity. Our approach is underpinned by a whole-school culture of safeguarding, where online safety is everyone's responsibility.

2.2 Aims and Objectives

The aims of this policy are to:

- Create and maintain a safe and supportive online environment for all members of the school community.
- Promote digital resilience, critical thinking, and responsible online behaviours among pupils and staff.
- Ensure compliance with all statutory and regulatory requirements relating to online safety, data protection, and safeguarding.
- Provide clear guidance on the safe and ethical use of technology, including emerging technologies such as artificial intelligence (AI).
- Equip staff, pupils, and parents/carers with the knowledge, skills, and confidence to recognise, respond to, and report online safety concerns.
- Foster effective partnerships with parents, carers, and external agencies to support a shared understanding of online safety.

2.3 Policy Principles

This policy is founded on the following principles:

- **A Whole-School Approach:** Online safety is embedded across all aspects of school life, including leadership, curriculum, staff development, and parental engagement.
- **Age-Appropriate Education:** Online safety education is tailored to the developmental stages and needs of pupils, ensuring relevance and accessibility.
- **Proactive Risk Management:** The school actively identifies, assesses, and mitigates online risks, including those arising from new technologies and emerging threats.
- **Inclusivity and Respect:** All members of the school community are entitled to learn and work in a safe, respectful, and inclusive digital environment.
- **Continuous Improvement:** Policy and practice are regularly reviewed and updated in response to new guidance, incidents, and stakeholder feedback.

3.0 Roles and Responsibilities

3.1 Governing Body and Leadership

The Governing Body and Headteacher hold strategic responsibility for online safety. They ensure that:

- The school has an effective, up-to-date online safety policy that complies with statutory requirements and is reviewed annually.
- Adequate resources are allocated for the implementation of online safety measures, including staff training, filtering and monitoring systems, and curriculum resources.
- Online safety is integrated into the school's safeguarding framework and self-evaluation processes
- Online safety is embedded in the school curriculum
- The effectiveness of the policy is monitored through regular reports from the Designated Safeguarding Lead (DSL) and safeguarding audits.
- The school responds promptly and appropriately to online safety incidents, including reporting to external agencies where required.

3.2 Designated Safeguarding Lead (DSL)

The DSL is the named lead for online safety and is responsible for:

- Leading the development, implementation, and review of the online safety policy.
- Coordinating the school's response to online safety incidents, including investigation, documentation, and liaison with external agencies.
- Ensuring all staff receive appropriate and up-to-date training on online safety, including emerging risks such as AI and social media.
- Maintaining accurate records of online safety incidents, staff training, and policy reviews.
- Supporting pupils, staff, and parents in understanding and responding to online safety concerns.
- Overseeing the effectiveness of filtering and monitoring systems and ensuring regular reviews are conducted.
- Ensuring online safety is included in safeguarding audits and self-evaluation.

3.3 Staff Responsibilities

All staff, including teaching, support, and administrative staff, are expected to:

- Model safe, responsible, and respectful online behaviours at all times.
- Embed online safety education within their teaching and interactions with pupils.
- Remain vigilant to signs of online risk, harm, or abuse, including cyberbullying, online sexual harassment, radicalisation, and risks associated with AI.
- Report any online safety concerns or incidents promptly to the DSL or appropriate member of the safeguarding team.
- Participate in mandatory induction and ongoing online safety training.
- Adhere to the school's Acceptable Use Agreements and ensure compliance with data protection requirements.
- Support pupils in developing digital resilience and critical thinking skills.

3.4 Pupil Responsibilities

Pupils are expected to:

- Use school technology and personal devices responsibly, safely, and respectfully, in line with the school's Acceptable Use Agreements.
- Report any online safety concerns, incidents, or inappropriate content to a trusted adult, teacher, or the DSL.
- Engage positively with online safety education and apply their learning to their online activities.
- Respect the privacy, dignity, and wellbeing of others in all online interactions.
- Seek help if they feel unsafe, threatened, or uncomfortable online, or if they witness harmful behaviour.

- Understand the importance of protecting their personal information and digital identity.

3.5 Parent/Carer Engagement

Parents and carers play a vital role in supporting their child's online safety. The school will:

- Provide regular information, guidance, and resources to help parents/carers understand online risks and support safe technology use at home.
- Offer workshops, newsletters, and online resources on current online safety issues, including managing screen time, social media, cyberbullying, and AI.
- Encourage open communication between home and school regarding online safety concerns.
- Involve parents/carers in policy review and development through consultation and feedback opportunities.
- Signpost parents/carers to reputable external sources of advice and support.

4.0 Policy Implementation

4.1 Whole-School Approach

Online safety is embedded across all aspects of school life at Inkpen Primary School. This includes:

- Leadership commitment to a culture of safeguarding, where online safety is prioritised in strategic planning and resource allocation.
- Integration of online safety into curriculum planning, pastoral support, and behaviour management.
- Regular communication and collaboration between staff, pupils, parents, and governors on online safety matters.
- Inclusion of online safety in school improvement planning, safeguarding audits, and self-evaluation processes.
- Engagement with external agencies, such as the local authority, police, and specialist organisations, to enhance practice and respond to emerging risks.

4.2 Staff Training and Awareness

All staff receive comprehensive online safety training as part of their induction and ongoing professional development. Training includes:

- Statutory and school-specific online safety responsibilities.
- Recognising and responding to online risks, including cyberbullying, online sexual harassment, radicalisation, and AI-related risks.
- Updates on emerging technologies, platforms, and trends, including generative AI, social media, and gaming.
- Procedures for reporting and managing online safety incidents.
- Data protection, privacy, and digital security.
- Use of filtering and monitoring systems and understanding their limitations.
- Promoting digital resilience and critical thinking in pupils.

Training is refreshed at least annually and whenever significant changes occur in statutory guidance or technology. Records of staff training are maintained and reviewed by the DSL.

4.3 Pupil Education and Curriculum Integration

Online safety education is delivered as part of the statutory computing curriculum (2014 National Curriculum) and is embedded across other subjects and pastoral programmes. Our curriculum follows the non-statutory guidance Teaching online safety in schools. Key features include:

- Age-appropriate, progressive online safety education, informed by frameworks such as UKCIS 'Education for a Connected World'.
- Coverage of key topics, including digital literacy, privacy, online reputation, cyberbullying, healthy relationships, misinformation, and the safe use of AI.
- Opportunities for pupils to develop critical thinking, digital resilience, and problem-solving skills.
- Use of real-life scenarios, interactive activities, and peer-led initiatives to engage pupils.
- Regular review and adaptation of curriculum content to address new and emerging risks.
- Support for pupils with additional needs or vulnerabilities, ensuring accessible and inclusive online safety education.

4.4 Parental Engagement and Education

The school recognises the importance of working in partnership with parents and carers to promote online safety. Strategies include:

- Regular communication through newsletters, emails, and the school website, highlighting current online safety issues and resources.
- Workshops and information sessions for parents/carers on topics such as social media, screen time, cyberbullying, and AI.
- Distribution of guidance materials, including Acceptable Use Agreements, online safety tips, and signposting to external support.

- Opportunities for parents/carers to provide feedback on the school's online safety provision and contribute to policy review.
- Collaboration with local agencies and organisations to support parental engagement and education.

5.0 Online Safety Risk Management

5.1 Risk Assessment Procedures

The school conducts regular risk assessments to identify, evaluate, and mitigate online risks. This includes:

- Annual review of online safety risks as part of the school's safeguarding audit.
- Ongoing monitoring of emerging threats, such as new social media platforms, online challenges, generative AI, and radicalisation.
- Consultation with staff, pupils, and parents to gather insights into online behaviours and concerns.
- Use of sector-standard tools, such as the SWGfL 360 Degree Safe self-review tool, to benchmark and improve practice.
- Implementation of targeted interventions and support for pupils or groups identified as at increased risk.
- Documentation of risk assessments and actions taken, with oversight by the DSL and Governing Body.

5.2 Filtering and Monitoring Systems

To protect pupils from harmful online content and activity, the school implements robust, age-appropriate filtering and monitoring systems, in line with KCSIE 2025 and DfE guidance: Meeting digital and Technology Standards in schools and colleges. This includes:

- Use of technical solutions to block access to inappropriate, illegal, or harmful content, including extremist material, online sexual abuse, and cyberbullying.
- Monitoring of online activity on school devices and networks to detect risky behaviours, safeguarding concerns, and breaches of Acceptable Use Agreements.
- Regular review and testing of filtering and monitoring systems to ensure effectiveness and adapt to new threats.
- Clear procedures for responding to alerts, including escalation to the DSL and, where necessary, external agencies.
- Documentation of filtering and monitoring procedures, reviews, and outcomes, with records maintained by the DSL.

- Communication with staff, pupils, and parents about the scope and limitations of filtering and monitoring, promoting shared responsibility for online safety.

5.3 Safe and Ethical Use of AI

The school recognises the opportunities and risks associated with the use of artificial intelligence (AI) in education as outlined in the Generative artificial intelligence in education. To ensure safe, ethical, and responsible use:

- All AI tools and systems used in school are subject to risk assessment, considering data privacy, safeguarding, and potential for misuse or bias.
- Staff and pupils receive training on the safe and ethical use of AI, including understanding its capabilities, limitations, and risks.
- Human oversight is maintained for all AI-driven processes, with clear accountability for decision-making.
- Procedures are in place to monitor AI systems for unintended consequences and to respond promptly to any concerns.
- Guidance is provided on the responsible use of generative AI, including issues of copyright, misinformation, and digital footprint.
- The school stays informed about developments in AI regulation and best practice, adapting policy and practice as required.

5.4 Data Protection and Privacy

The school is committed to protecting the personal data and privacy of all members of the school community, in accordance with the Data Protection Act 2018 and UK GDPR. This includes:

- Implementing privacy by design in all digital systems and processes.
- Ensuring that personal data is collected, stored, processed, and shared securely and lawfully.
- Providing staff and pupils with guidance on protecting their own and others' personal information online.
- Conducting data protection impact assessments for new technologies and systems, including AI tools.
- Responding promptly to data breaches or privacy concerns, in line with statutory reporting requirements.
- Ensuring that third-party providers of digital services comply with data protection standards.

6.0 Responding to Online Safety Incidents

6.1 Reporting Procedures

The school provides clear, accessible routes for reporting online safety concerns or incidents. These include:

- Pupils can report concerns to any trusted adult, teacher, or directly to the DSL, either in person or via confidential reporting systems.
- Staff must report all online safety concerns, incidents, or breaches of Acceptable Use Agreements to the DSL or Headteacher without delay.
- Parents/carers are encouraged to report concerns to the DSL, Headteacher, or class teacher, either in person, by phone, or via email.
- All reports are treated seriously, with respect for confidentiality and the welfare of those involved.
- Where required, the school will report incidents to external agencies, such as the local authority, police, or the Local Safeguarding Partnership, in line with statutory obligations.

6.2 Incident Management and Response

When an online safety incident occurs, the school will:

- Take immediate steps to ensure the safety and wellbeing of those involved.
- Investigate the incident thoroughly, gathering relevant evidence and statements.
- Record the incident, actions taken, and outcomes using the Online Safety Incident Report Form.
- Provide appropriate support to victims, including pastoral care, counselling, and involvement of external agencies where necessary.
- Take proportionate disciplinary action against those responsible, in line with the Behaviour and Anti-Bullying policies.
- Review the incident to identify lessons learned and inform improvements to policy and practice.
- Communicate with parents/carers as appropriate, ensuring transparency and support.
- Record the incident on CPOMS with the appropriate actions

Specific types of incidents, such as cyberbullying, online sexual harassment, radicalisation, or data breaches, will be managed in accordance with relevant statutory guidance and school policies.

6.3 Recording, Documentation, and Review

Accurate and comprehensive records are maintained for all online safety incidents using the Online Safety Incident Report form. The following will be included:

- Details of the incident, those involved, actions taken, and outcomes.
- Interventions and support provided to pupils or staff.
- Communication with parents/carers and external agencies.
- Review of incidents to identify trends, emerging risks, and areas for improvement.

The DSL is responsible for ensuring that records are kept secure, up to , date, reviewed regularly, and used to inform safeguarding practice and policy development.

7.0 Categories of online safeguarding concerns

7.1 Cyberbullying

Cyberbullying can include the following:

- Threatening, intimidating, or upsetting text messages
- Threatening or embarrassing pictures and video clips sent via mobile phone cameras
- Silent or abusive phone calls or using the victim's phone to harass others, to make them think the victim is responsible
- Threatening or bullying emails, possibly sent using a pseudonym or someone else's name
- Menacing or upsetting responses to someone in a chatroom
- Unpleasant messages sent via instant messaging
- Unpleasant or defamatory information posted to blogs, personal websites and social networking sites, e.g. Facebook, Twitter, Instagram, TikTok etc.

Cyberbullying against pupils or staff is not tolerated under any circumstances. Incidents of cyberbullying are dealt with quickly and effectively wherever they occur in line with the Antibullying Policy.

7.2 Child on child sexual abuse and harassment

Pupils may also use the internet and technology as a vehicle for sexual abuse and harassment. Staff will understand that this abuse can occur both in and outside of school and off and online and will remain aware that pupils are less likely to report concerning online sexual behaviours, particularly if they are using websites that they know adults will consider to be inappropriate for their age.

The following are examples of online harmful sexual behaviour of which staff will be expected to be aware:

- Threatening, facilitating or encouraging sexual violence

- Upskirting, i.e. taking a picture underneath a person's clothing without consent and with the intention of viewing their genitals, breasts or buttocks
- Sexualised online bullying, e.g. sexual jokes or taunts
- Unwanted and unsolicited sexual comments and messages
- Consensual or non-consensual sharing of sexualised imagery

Staff will be aware that creating, possessing, and distributing indecent imagery of other children, i.e. individuals under the age of 18, is a criminal offence, even where the imagery is created, possessed, and distributed with the permission of the child depicted, or by the child themselves.

The school responds to all concerns regarding online child on child sexual abuse and harassment, regardless of whether the incident took place on the school premises or using school-owned equipment. Concerns regarding online child on child abuse are reported to the DSL, who will investigate the matter in line with the Behaviour Policy and the Child Protection and Safeguarding Policy.

7.3 Grooming and exploitation

Grooming

Grooming is defined as the situation whereby an adult builds a relationship, trust and emotional connection with a child with the intention of manipulating, exploiting and/or abusing them.

- Staff will be aware that grooming often takes place online and that pupils who are being groomed are commonly unlikely to report this behaviour for many reasons, including the following:
- The pupil believes they are talking to another child, when they are actually talking to an adult masquerading as someone younger with the intention of gaining their trust to abuse them.
- The pupil does not want to admit to talking to someone they met on the internet for fear of judgement, feeling embarrassed, or a lack of understanding from their peers or adults in their life.
- The pupil may have been manipulated into feeling a sense of dependency on their groomer due to the groomer's attempts to isolate them from friends and family.
- Talking to someone secretly over the internet may make the pupil feel 'special', particularly if the person they are talking to is older.
- The pupil may have been manipulated into feeling a strong bond with their groomer and may have feelings of loyalty, admiration, or love, as well as fear, distress and confusion.

Due to the fact pupils are less likely to report grooming than other online offences, it is particularly important that staff understand the indicators of this

type of abuse. The DSL will ensure that online safety training covers online abuse, the importance of looking for signs of grooming and what the signs of online grooming are, including:

- Being secretive about how they are spending their time.
- Having an older boyfriend or girlfriend, usually one that does not attend the school and whom their close friends have not met.
- Having money or new possessions, e.g. clothes and technological devices, that they cannot or will not explain.

7.4 Child sexual exploitation (CSE) and child criminal exploitation (CCE)

Although CSE often involves physical sexual abuse or violence, online elements may be prevalent, e.g. sexual coercion and encouraging children to behave in sexually inappropriate ways through the internet. In some cases, a pupil may be groomed online to become involved in a wider network of exploitation, e.g. the production of child pornography or forced child prostitution and sexual trafficking.

CCE is a form of exploitation in which children are forced or manipulated into committing crimes for the benefit of their abuser, e.g. drug transporting, shoplifting and serious violence. While these crimes often take place in person, it is increasingly common for children to be groomed and manipulated into participating through the internet.

Where staff have any concerns about pupils with relation to CSE or CCE, they will bring these concerns to the DSL without delay, who will manage the situation in line with the Child Protection and Safeguarding Policy.

7.5 Radicalisation

Radicalisation is the process by which a person comes to support terrorism and extremist ideologies associated with terrorist groups. This process can occur through direct recruitment, e.g. individuals in extremist groups identifying, targeting and contacting young people with the intention of involving them in terrorist activity, or by exposure to violent ideological propaganda. Children who are targets for radicalisation are likely to be groomed by extremists online to the extent that they believe the extremist has their best interests at heart, making them more likely to adopt the same radical ideology.

Staff members will be aware of the factors which can place certain pupils at increased vulnerability to radicalisation, as outlined in the British Values Policy and as a result of their annual PREVENT training. Staff will be expected to exercise vigilance towards any pupils displaying indicators that they have been, or are being, radicalised.

Where staff have a concern about a pupil relating to radicalisation, they will report this to the DSL without delay, who will handle the situation in line with the British Values Policy. All staff and Governors will undertake Prevent training. Training registers are kept ensuring this is all kept up to date.

7.5 Mental health

The internet, particularly social media, can be the root cause of a number of mental health issues in pupils, e.g. low self-esteem and suicidal ideation.

Staff will be aware that online activity both in and outside of school can have a substantial impact on a pupil's mental state, both positively and negatively. The DSL will ensure that training is available to help ensure that staff members understand popular social media sites and terminology, the ways in which social media and the internet in general can impact mental health, and the indicators that a pupil is suffering from challenges in their mental health.

7.6 Online hoaxes and harmful online challenges

For the purposes of this policy, an "online hoax" is defined as a deliberate lie designed to seem truthful, normally one that is intended to scaremonger or to distress individuals who come across it, spread on online social media platforms. This risk has increased due to the use of AI.

For the purposes of this policy, "harmful online challenges" refers to challenges that are targeted at young people and generally involve users recording themselves participating in an online challenge, distributing the video through social media channels, and daring others to do the same. Although many online challenges are harmless, an online challenge becomes harmful when it could potentially put the participant at risk of harm, either directly because of partaking in the challenge itself or indirectly as a result of the distribution of the video online – the latter will usually depend on the age of the pupil and the way in which they are depicted in the video.

Where staff suspect there may be a harmful online challenge or online hoax circulating amongst pupils in the school, they will report this to the DSL immediately.

The DSL will conduct a case-by-case assessment for any harmful online content brought to their attention, establishing the scale and nature of the possible risk to pupils, and whether the risk is one that is localised to the school or the local area, or whether it extends more widely across the country. Where the harmful content is prevalent mainly in the local area, the DSL will consult with the LA about whether quick local action can prevent the hoax or challenge from spreading more widely.

Prior to deciding how to respond to a harmful online challenge or hoax, the DSL and the headteacher will decide whether each proposed response is:

- In line with any advice received from a known, reliable source, e.g. the UK Safer Internet Centre, when fact-checking the risk of online challenges or hoaxes.
- Careful to avoid needlessly scaring or distressing pupils.
- Not inadvertently encouraging pupils to view the hoax or challenge where they would not have otherwise come across it, e.g. where content is explained to younger pupils but is almost exclusively being shared amongst older pupils.
- Proportional to the actual or perceived risk.
- Helpful to the pupils who are, or are perceived to be, at risk.
- Appropriate for the relevant pupils' age and developmental stage.
- Supportive.
- In line with the Child Protection and Safeguarding Policy.

Where the DSL's assessment finds an online challenge to be putting pupils at risk of harm, e.g. it encourages children to participate in age-inappropriate activities that could increase safeguarding risks or become a child protection concern, they will ensure that the challenge is directly addressed to the relevant pupils, e.g. those within a particular age range that is directly affected or even to individual children at risk where appropriate.

The DSL/headteacher will only implement a school-wide approach to highlighting potential harms of a hoax or challenge when the risk of needlessly increasing pupils' exposure to the risk is considered and mitigated as far as possible.

7.7 Cyber-crime

Cyber-crime is criminal activity committed using computers and/or the internet. There are two key categories of cyber-crime:

- Cyber-enabled – these crimes can be carried out offline; however, are made easier and can be conducted at higher scales and speeds online, e.g. fraud, purchasing and selling of illegal drugs, and sexual abuse and exploitation.
- Cyber-dependent – these crimes can only be carried out online or by using a computer, e.g. making, supplying or obtaining malware, illegal hacking, and 'booting', which means overwhelming a network, computer or website with internet traffic to render it unavailable.

The school will factor into its approach to online safety the risk that pupils with a particular affinity or skill in technology may become involved, whether deliberately or inadvertently, in cyber-crime. Where there are any concerns

about a pupil's use of technology and their intentions with regard to using their skill and affinity towards it, the DSL will consider a referral to the Cyber Choices programme, which aims to intervene where children are at risk of committing cyber-crime and divert them to a more positive use of their skills and interests.

The DSL/headteacher will ensure that pupils are taught, throughout the curriculum, how to use technology safely, responsibly and lawfully, and will ensure that pupils cannot access sites or areas of the internet that may encourage them to stray from lawful use of technology, e.g. the 'dark web', on school-owned devices or on school networks through the use of appropriate firewalls.

8.0 Monitoring, Evaluation, and Review

8.1 Policy Monitoring and Self-Evaluation

The effectiveness of the online safety policy is monitored through:

- Regular safeguarding audits, including review of online safety provision, incident records, and staff training.
- Use of self-evaluation tools, such as SWGfL 360 Degree Safe, to benchmark practice and identify areas for development.
- Analysis of incident data to identify trends, recurring issues, and the impact of interventions.
- Feedback from staff, pupils, parents, and governors on the effectiveness of online safety education and support.
- External review and challenge, including input from the Local Safeguarding Partnership and Ofsted inspection.

8.2 Policy Review Process

This policy is reviewed annually, or sooner if required by changes in statutory guidance, legislation, or significant incidents. The review process includes:

- Consultation with staff, pupils, parents, and governors to gather feedback and suggestions for improvement.
- Review of new and emerging risks, technologies, and statutory requirements.
- Updating of procedures, resources, and training in response to lessons learned.
- Ratification of the revised policy by the Governing Body, with updated versions disseminated to all stakeholders.

8.3 Continuous Improvement

The school is committed to continuous improvement in online safety practice. This is achieved by:

- Learning from incidents, audits, and stakeholder feedback to refine policy and procedures.
- Keeping up to date with developments in technology, statutory guidance, and best practice.
- Investing in staff development, resources, and partnerships to enhance online safety provision.
- Celebrating successes and sharing good practice within the school and with the wider community.

9.0 Communication and Accessibility

9.1 Policy Dissemination

The Online Safety Policy is communicated to all members of the school community through:

- Publication on the school website and inclusion in staff and parent handbooks.
- Induction packs for new staff, volunteers, and governors.
- Staff meetings, training sessions, and briefings.
- Pupil assemblies, lessons, and pastoral sessions.
- Display of key messages and reporting routes around the school.
- Sharing with visitors and contractors as appropriate.

9.2 Accessibility and Inclusion

The school is committed to ensuring that this policy is accessible to all members of the community, including those with additional needs or for whom English is an additional language. This includes:

- Providing the policy in alternative formats or languages on request.
- Using clear, jargon-free language and visual aids to support understanding.
- Adapting online safety education and resources to meet the needs of pupils with SEND or other vulnerabilities.
- Consulting with pupils, parents, and staff to ensure accessibility and inclusivity.

10.0 Related Policies and Links

This policy should be read in conjunction with the following related policies and documents:

- **Safeguarding and Child Protection Policy:** Procedures for safeguarding pupils, including online risks.
- **Behaviour Policy:** Expectations for conduct, including online behaviour and use of technology.
- **Anti-Bullying Policy:** Prevention and management of bullying, including cyberbullying.
- **Data Protection Policy:** Compliance with the Data Protection Act 2018 and UK GDPR.
- **Acceptable Use Agreements (AUA):** Expectations for safe and responsible use of technology by staff, pupils, and parents.
- **Staff Code of Conduct:** Professional standards for staff, including online interactions.
- **Remote Learning Policy:** Safe use of technology for remote and blended learning.
- **Whistleblowing Policy:** Reporting concerns about safeguarding or online safety.

External Guidance and Resources:

- Department for Education (DfE) Guidance on Online Safety
- Keeping Children Safe in Education (KCSIE) 2025
- UK Council for Internet Safety (UKCIS) 'Education for a Connected World'
- National Cyber Security Centre (NCSC) Cyber Security for Schools
- SWGfL 360 Degree Safe self-review tool
- Local Safeguarding Partnership guidance
- Child Exploitation and Online Protection Centre (CEOP)
- Internet Matters, Childnet, NSPCC, and other reputable online safety organisations
- PEGI age rating for gaming

11.0 Appendices

- **11.1 Acceptable Use Agreements (AUA) KS 1 and 2**
- **11.2 Online Safety Incident Report Form**
- **11.3 Filtering and Monitoring Log**

11.1 Acceptable Use Agreements (AUA)

KS1 AUA

Inkpen Primary School
Aiming high

This acceptable use agreement is intended to ensure:

- that community users of school digital technologies will be responsible users and stay safe while using these systems and devices
- that school systems, devices and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that users are protected from potential harm in their use of these systems and devices

I understand that I must use school systems and devices in a responsible way, to ensure that I am safe and that others are safe online.

I agree that I will:

- Only open pages which my teacher says are OK;
- Only work with people I know in real life;
- Tell my teacher if anything makes me feel scared or uncomfortable;
- Make sure all messages I send are polite;
- Show my teacher if I get a nasty message;
- Not reply to any nasty message or anything which makes me feel uncomfortable;
- Talk to my teacher before using anything on the internet;
- Not play games (unless told to by my teacher) during lesson time;
- Not tell people about myself online (I will not tell them my name, anything about my family and home, phone numbers or pets);
- Not load photos of myself onto the computer;
- Never agree to meet a stranger. Remember that anything I do on the computer may be seen by someone else. I have discussed these rules with my child and they understand what is expected from them and know what to do when there is an issue.
- Not share any of my passwords with anyone else

I have discussed these rules with my child and they understand what is expected from them and know what to do when there is a problem.

Pupil's name ..... Class.....

Signed..... Date.....

Signed.....(parent/carer) Date.....

KS2 AUA

11.1 Acceptable Use Agreements (AUA) KS2

Inkpen Primary School
Aiming high

This acceptable use agreement is intended to ensure:

- that community users of school digital technologies will be responsible users and stay safe while using these systems and devices
- that school systems, devices and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that users are protected from potential harm in their use of these systems and devices

I understand that I must use school systems and devices in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems, devices and other users.

- I understand that I am not permitted to bring personal devices from home into school. ***In emergencies only, and in agreement with the headteacher, phones may be brought in and handed to the school office.***
- I will only use the school's computers for schoolwork and homework, unless permission has been given by the teacher;
- I will only edit or delete my own files and not look at, or change, other people's files without their permission;
- I will keep my logins and passwords secret;
- I will not bring files into school without permission or upload inappropriate material to my workspace;
- I am aware that some websites and social networks have age restrictions and I should respect this;
- I will not attempt to visit Internet sites that I know to be banned by the school;
- I will only email people I know, or those 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 will never arrange to meet someone I have only ever previously met on the Internet, unless my parent/carer has given me permission and I take a responsible adult with me;
- 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 understood these rules and agree to them.

Pupil's name ..... Class.....

Signed..... Date.....

Signed.....(parent/carer) Date.....

11.2 Online Safety Incident Report Form

Inkpen Primary School

Online Safety Incident Report Form

Date and time of incident:
Nature of incident:
Actions taken:
Communication with parents:
Communication with external agencies:
Signed: (Adult reporting incident)
Signed: (DSL/Headteacher)

11.3 Filtering and Monitoring Log

Inkpen Primary School

Filtering test record

Date and time filtering test run:
Results of test:
Any concerns:
Actions required:
Communication with external agencies:
Signed: (Adult running test)
Signed: (DSL/Headteacher)