Knowsley Junior School

E-Safety Policy

Introduction

Knowsley Junior School is committed to safeguarding and promoting the welfare of our pupils in all aspects of their use of digital technologies. This E-Safety Policy outlines our approach to ensuring that pupils are safe and responsible users of technology, in line with current UK guidance (KCSIE 2025) and Ofsted requirements.

The policy highlights the integration of Purple Mash, Kapow, and CEOP resources in our E-Safety education, supporting pupils from Years 3 to 6 to navigate the online world safely.

Policy Aims:

- Protect and educate pupils in their use of technology.
- Establish mechanisms to identify, intervene, and escalate online incidents.
- Ensure all members of the school community understand their roles and responsibilities.
- Promote a culture of responsible, safe, and ethical technology use.
- Address emerging online risks such as social media, gaming, AI content, and online radicalisation.

Roles and Responsibilities:

Governing Body:

- Ensure effective E-Safety policies and procedures are in place.
- Monitor and review policy effectiveness annually.

Head teacher:

- Implement the policy across the school.
- Provide staff training and resources to support E-Safety education.
- Promote a positive culture of online safety school-wide.

E-Safety Coordinator:

- Oversee E-Safety practices and audit the school's systems regularly.
- Advise staff on E-Safety issues.
- Liaise with IT support to maintain filtering and monitoring systems.
- Report findings and trends to the Headteacher and Governing Body.
- Designated Safeguarding Lead (DSL)
- Work with the E-Safety Coordinator to address online safety incidents with safeguarding implications.
- Ensure E-Safety is embedded in the school's safeguarding strategy.

Staff:

- Embed E-Safety in teaching and model responsible digital behaviour.
- Report all online incidents promptly.
- Participate in annual E-Safety training and updates.
- Pupils
- Follow the school's online safety rules.
- Report concerns about online content or behaviour.

- Engage positively with E-Safety education.

Parents/Carers:
- Support the school's E-Safety approach at home.
- Reinforce safe internet practices.
- Attend workshops and use school-provided resources.

Education and Training

Pupils:
- E-Safety is integrated into computing, PSHE, and dedicated activities.
- Purple Mash and Kapow provide age-appropriate lessons and interactive activities.
- CEOP resources and the CEOP button are used to educate pupils on reporting concerns.
- Key topics include online privacy, cyberbullying, social media, digital footprints, AI content, gaming safety, and reporting harmful behaviour.

Staff:
- Annual training on current E-Safety trends and emerging risks.
- Guidance on using Purple Mash, Kapow, and CEOP effectively.
- Regular updates on handling online incidents and safeguarding concerns.

Parents/Carers:
- Provided resources support understanding of online risks and safe practices at home.
- Guidance on parental controls, monitoring, and using the CEOP button.
- Links to trusted online safety sites (e.g., UK Safer Internet Centre, NSPCC).

Platforms and Resources

Purple Mash
- Interactive lessons, quizzes, and activities promoting safe online behaviour.
- Encourages critical thinking about technology use.

Kapow
- Comprehensive E-Safety curriculum within PSHE.
- Emphasises real-life scenarios and problem-solving.

CEOP
- Educates pupils on reporting inappropriate or harmful behaviour online.
- CEOP button is clearly accessible on the school website and platforms.

Technical Infrastructure:
- Network is protected by filtering and monitoring to block inappropriate content.
- Regular reviews and updates to maintain security against emerging threats.
- Secure passwords and user authentication protect personal and sensitive data.
- Procedures are in place for safe remote learning, including secure video calls and monitored platforms.

Incident Management:

- Clear reporting and escalation procedures are followed for all online safety incidents.
- The E-Safety Coordinator logs incidents and liaises with the DSL for safeguarding concerns.
- Pupils involved receive guidance and support, with preventative measures implemented.
- Regular review of incident logs to identify trends and improve E-Safety practices.

Monitoring and Evaluation:
- Regular audits of systems, teaching, and incident logs to assess effectiveness.
- Pupil surveys and classroom feedback inform improvements.
- Policy updates address new technologies and emerging online risks.

Data Protection:
- All personal data is handled in line with the school's Data Protection Policy and GDPR requirements.
- Staff, pupils, and parents sign Acceptable Use Agreements upon starting at Knowsley Junior School.
- Electronic and paper records are securely stored and only accessed by authorised staff.

Policy Review:
- Reviewed annually by the E-Safety Coordinator, Headteacher, and Governing Body.
- Feedback from pupils, staff, and parents is incorporated.
- Updates are made in response to emerging risks, technological change, or legal guidance.

Related Policies:
- Child Protection and Safeguarding Policy
- Anti-Bullying Policy
- Behaviour Policy
- Data Protection Policy
- Acceptable Use Policy (AUP)
- Remote Learning Policy

Knowsley Junior School is dedicated to ensuring the online safety of pupils. Through the effective use of Purple Mash, Kapow, CEOP resources, secure technology, and robust training, we provide a safe, responsible, and supportive digital environment for all pupils to thrive.

Data Protection

The procedures and practice created by this policy have been reviewed in the light of our Data Protection Policy.

All data will be handled in accordance with the school's Data Protection Policy.

What ?	Probable Content	Why ?	Who ?	Where ?	When ?
Staff Acceptable Use Agreements	Names and signatures confirming understanding of E-Safety responsibilities	To ensure staff follow E-Safety procedures and safeguarding guidance	All teaching and support staff	Paper staff file / electronic copy on secure server	Upon joining / reviewed annually
Pupil Acceptable Use Agreements	Pupil names, class, signatures confirming safe technology use	To ensure pupils understand how to use school technology safely	Class teachers / Computing Lead	Paper copy in classroom / electronic copy on secure server	Start of school year or on entry
Parental Consent Forms	Parent names and signatures for consent to access online learning platforms	To comply with GDPR and ensure parental agreement	Class teachers / Computing Lead	Paper copy in classroom / electronic copy on secure server	On entry or start of year
E-Safety Incident Logs	Summary of incidents, pupils/staff involved, actions taken	To monitor incidents, safeguard pupils, and identify trends	E-Safety Coordinator / DSL	Secure digital log / safeguarding files	Ongoing; reviewed termly

As such, our assessment is that this policy :

Has Few / No Data Compliance Requirements	Has A Moderate Level of Data Compliance Requirements	Has a High Level Of Data Compliance Requirements
		✓

Signed Chair of Governors …….

Date: ……/……/…….

Review Date: ……..……...